# XenApp und XenDesktop 7.9

Aug 17, 2016


## Neue Funktionen

Behobene Probleme

Bekannte Probleme

Nicht in diesem Release enthaltene Features

Hinweise zu Drittanbietern

## Systemanforderungen

## Technische Übersicht

Konzepte und Komponenten

Active Directory

Datenbanken

Bereitstellungsmethoden

Referenzarchitekturen

Designanleitungen

Implementierungsanleitungen

## Installation und Konfiguration

Vorbereiten der Installation

Installieren über die grafische Oberfläche

Installieren über die Befehlszeile

Installieren von VDAs mit Skripts

Installieren von VDAs unter Red Hat Linux

Installieren von VDAs mit SUSE Linux

Erstellen einer Site

Erstellen von Maschinenkatalogen

Verwalten von Maschinenkatalogen

Erstellen von Bereitstellungsgruppen

Verwalten von Bereitstellungsgruppen

Erstellen von Anwendungsgruppen

Verwalten von Anwendungsgruppen


 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Remote-PC-Zugriff

App-V

AppDisks

Lokaler App-Zugriff und URL-Umleitung

XenApp Secure Browser

Server-VDI

Personal vDisk

Entfernen von Komponenten

## Upgrades und Migration

Upgrade einer Bereitstellung

Migrieren von XenApp 6.x

Migrieren von XenDesktop 4

## Sicherheit

Sicherheit – Überlegungen und bewährte Methoden

Delegierte Administration

Smartcards

Transport Layer Security (TLS)

Federated Authentication Service

## Drucken

Beispiel einer Druckkonfiguration

Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge

Druckrichtlinien und -einstellungen

Bereitstellen von Druckern

Pflege der Druckumgebung

## HDX

Thinwire-Kompatibilitätsmodus

Framehawk Virtual Channel

HDX 3D Pro

Flash-Umleitung

GPU-Beschleunigung für Windows Desktopbetriebssysteme

GPU-Beschleunigung für Windows-Serverbetriebssystem

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

OpenGL Software Accelerator

Audiofeatures

Prioritäten für den Netzwerkdatenverkehr

Überlegungen zu USB und Clientlaufwerk

## Richtlinien

Arbeiten mit Richtlinien

Richtlinienvorlagen

Erstellen von Richtlinien

Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien

Standardrichtlinieneinstellungen

Referenz für Richtlinieneinstellungen

## Verwaltung

Lizenzierung

Anwendungen

Zonen

Verbindungen und Ressourcen

Verbindungsleasing

Virtuelle IP-Adressen und virtuelles Loopback

Delivery Controller

Sitzungen

Verwenden der Suche in Studio

Tags

Unterstützung für IPv4/IPv6

Clientordnerumleitung

Benutzerprofile

Citrix Insight Services

## Überwachung

Sitzungsaufzeichnung

Konfigurationsprotokollierung

Überwachen von Personal vDisks

## Director

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Erweiterte Konfiguration

Überwachen von Bereitstellungen

Warnungen und Benachrichtigungen

Delegierte Administration und Director

Sichere Bereitstellung von Director

Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7

Konfigurieren von HDX Insight

Behandeln von Benutzerproblemen

SDKs und APIs

Überwachungsdienst-OData-API

FIPS-Beispielbereitstellungen

Citrix SCOM Management Pack für XenApp und XenDesktop

Citrix SCOM Management Pack für den Lizenzserver

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# Neue Funktionen

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:

Info zu diesem Release

XenApp und XenDesktop 7.9

Virtual Delivery Agents 7.9

StoreFront 3.6

Provisioning Services 7.9

AppDNA 7.9

# Info zu diesem Release

Release 7.9 von XenApp und XenDesktop enthält neue Versionen der Windows-VDAs und einiger XenApp- und XenDesktop-Kernkomponenten. Sie haben folgende Möglichkeiten:

- **Installieren oder Aktualisieren einer XenApp- oder XenDesktop-Site**

  Installieren oder aktualisieren Sie alle Kernkomponenten und Virtual Delivery Agents (VDAs) mit der ISO-Datei. Dadurch können Sie alle aktuellen Features (s. u.) verwenden. Weitere Informationen finden Sie im Artikel Vorbereiten der Installation bzw. Upgrade einer Bereitstellung.

- **Installieren oder Aktualisieren von VDAs einer vorhandenen Site**

  Wenn Sie eine XenApp- oder XenDesktop-Bereitstellung haben und noch kein Upgrade der Kernkomponenten durchführen können, können Sie durch eine Installation eines VDAs bzw. ein Upgrade auf den aktuellen VDA die aktuellen HDX-Features verwenden. Dies ist beispielsweise nützlich, wenn Sie die Erweiterungen in einer Testumgebung testen möchten. Eine Zusammenfassung der neuen und aktualisierten Features der VDAs finden Sie weiter unten. Anweisungen finden Sie in folgenden Artikeln:

  Installieren/Upgrade von VDAs mit der grafischen Oberfläche des eigenständigen VDA-Installationsprogramms

  Installieren/Upgrade von VDAs mit der Befehlszeilenschnittstelle des eigenständigen VDA-Installationsprogramms

Die XenApp- und XenDesktop-Downloadseiten für dieses Release enthalten auch aktualisierten Versionen der folgenden Software. Weitere Informationen zu Features und Installationsanweisungen finden Sie in der Dokumentation der jeweiligen Komponente.

StoreFront

Provisioning Services

AppDNA

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# XenApp und XenDesktop 7.9

Das Produktrelease enthält die nachfolgend aufgeführten neuen und erweiterten Features.

## Installation und Konfiguration

In diesem Abschnitt werden die Änderungen in diesem Release bei der Installation und Konfiguration von XenApp und XenDesktop zusammengefasst.

- Analysedaten werden bei der Installation von Komponenten gesammelt und lokal gespeichert.
- Wenn Sie einen VDA installieren und keine Controlleradressen angeben, werden Sie daran erinnert, dass der VDA sich nur registrieren kann, wenn Controlleradressen angegeben werden.
- Wenn Sie bei der Installation eines VDA mindestens eine Controlleradresse angeben, überprüft das Installationsprogramm, ob eine Verbindung zwischen VDA und Controller hergestellt werden kann und meldet das Ergebnis.
- Die Installationsassistenten bieten die Teilnahme am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit nicht mehr an, da die Teilnahme angenommen wird.
- Die Installationsassistenten für Kernkomponenten und VDA bieten nun die Registrierung für Call Home.
- Sie können jetzt den Verbundauthentifizierungsdienst über die grafische Benutzeroberfläche des Produktinstallationsprogramms installieren.

Die folgenden Änderungen wurden für die mögliche Verwendung in zukünftigen Releases implementiert.

- Microsoft SQL Express LocalDB 2014 wird automatisch installiert, wenn Sie einen Delivery Controller installieren. Diese Software wird nicht für die Site-, Überwachungs- und Protokollierungsdatenbanken verwendet. Es gibt keine Administratorinteraktion mit der Datenbank. Wenn Sie die Installation verhindern möchten, installieren Sie den Controller mit dem Befehl "XenDesktopServerSetup.exe" mit der Option /exclude "Microsoft SQL Server 2014 Express LocalDB".
- Wenn Sie beim Erstellen einer Site die SQL Server Express-Datenbank zur Verwendung als Sitedatenbank installieren (dies ist die Standardeinstellung), wird nach der Installation der Datenbanksoftware ein Neustart ausgeführt. Der Neustart wird nicht ausgeführt, wenn Sie die SQL Server Express-Software zur Verwendung als Sitedatenbank nicht installieren.

## Upgrades

Bei einem Upgrade erkennt das Installationsprogramm folgende Komponenten nicht mehr und aktualisiert sie auch nicht mehr: Citrix Receiver für Windows Enterprise, das Offline Plug-In für Windows und das XenApp Plug-In für gestreamte Anwendungen. Weitere Informationen hierzu finden Sie im Artikel Upgrade einer Bereitstellung.

## Provisioning: MCS-Speicheroptimierung für I/O

Wenn Sie eine Verbindung zu einem Hypervisor oder Clouddienstanbieter zum Hosten von Maschinen erstellen, die mit Maschinenerstellungsdienste (MCS) erstellt wurden, können Sie nun Speicherorte für die verschiedenen Datentypen angeben:

- Betriebssystemdaten, einschließlich Masterimages.
- Temporäre Daten, einschließlich aller nicht persistenten Daten, die auf mit MSC bereitgestellten Maschinen geschrieben werden, Windows-Seitendateien, Benutzerprofildaten und alle Daten, die mit ShareFile synchronisiert werden. Diese Daten werden beim Neustart einer Maschine verworfen.
- Persönliche Daten, die auf persönlichen vDisks gespeichert werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Durch die Bereitstellung von separatem Speicher für die einzelnen Datentypen können Sie auf Speichergeräten die Last reduzieren und die IOPS-Leistung verbessern und so den größten Nutzen aus den verfügbaren Ressourcen des Hosts ziehen. Außerdem kann so der entsprechende Speicher für die verschiedenen Datentypen verwendet werden, denn Persistenz und Resilienz ist für einige Daten wichtiger als für andere.

Wenn Sie für Hypervisors freigegebenen Speicher wählen, können Sie auch wählen, ob Sie lokalen Speicher für temporäre Maschinendaten verwenden. Wenn Sie einen Maschinenkatalog erstellen, der diese Verbindung verwendet, können Sie für die Größe von Cachedatenträger und Speicher aller VMs andere als die Standardwerte aktivieren und konfigurieren.

Bei der Auswahl von lokalem Speicher für den Hypervisor können Sie wählen, ob Sie freigegebenen Speicher für persönliche vDisks verwenden (wenn Sie persönliche vDisks).

Weitere Informationen finden Sie in den Artikeln Verbindungen und Ressourcen und Erstellen von Maschinenkatalogen.

### Provisioning: Integration von Nutanix in Studio

Wenn Sie Nutanix Acropolis zum Hosten von bereitgestellten VMs verwenden, installieren Sie das Nutanix Plug-In auf den Delivery Controllern, um die Konfiguration von Nutanix-Verbindungen in Studio zu ermöglichen.

Wenn Sie mit Studio eine Verbindung zu Nutanix und einem Maschinenkatalog erstellen, der ein Nutanix-Image verwendet, können Sie mit dem Assistenten sowohl Standard- als auch Nutanix-spezifische Konfigurationsinformationen angeben.

Weitere Informationen finden Sie im Artikel Nutanix-Virtualisierungsumgebungen.

### Veröffentlichen: Anwendungsgruppen

Mit Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die von verschiedenen Bereitstellungsgruppen gemeinsam verwendet werden oder die von einer Untergruppe von Benutzern in den Bereitstellungsgruppen verwendet werden.

Anwendungsgruppen sind optional. Sie bieten eine Alternative dazu, dieselben Anwendungen mehreren Bereitstellungsgruppen hinzuzufügen. Bereitstellungsgruppen können mehr als einer Anwendungsgruppe zugeordnet sein und eine Anwendungsgruppe kann mehr als einer Bereitstellungsgruppe zugeordnet sein.

Weitere Informationen finden Sie in den Artikeln Erstellen von Anwendungsgruppen und Verwalten von Anwendungsgruppen.

Die Einführung von Anwendungsgruppen wirkt sich auf mehrere andere Studio-Bereiche aus. Wenn Sie beispielsweise die Eigenschaften einer Anwendung bearbeiten, kann die Gruppenmitgliedschaft Bereitstellungsgruppen und/oder Anwendungsgruppen umfassen. Zuvor musste eine Anwendung mindestens einer Bereitstellungsgruppe zugeordnet sein, jetzt muss sie mit mindestens eine Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Weitere Informationen zur Verwaltung von Anwendungen finden Sie unter Anwendungen.

### Sicherheit und Zugriff: Federated Authentication Service

Der Citrix Federated Authentication Service ist eine privilegierte Komponente für die Integration mit der Microsoft Zertifizierungsstelle. Der Dienst stellt dynamisch Zertifikate für Benutzer aus, sodass diese sich bei einer Citrix Umgebung so anmelden können, als hätten sie eine Smartcard. Dadurch kann in StoreFront eine größere Bandbreite an Authentifizierungsoptionen, darunter z. B. SAML-Assertionen (Security Assertion Markup Language), verwendet werden.

Weitere Informationen finden Sie im Artikel Federated Authentication Service.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Citrix Insight Services

Weitere Informationen über die Telemetriefeatures, einschließlich der Teilnahmeoptionen, finden Sie im Artikel Citrix Insight Services.

**Analysefeatures des Produktinstallationsprogramms**

Bei Verwendung des Produktinstallationsprogramms werden Analysedaten gesammelt und lokal gespeichert, wenn Sie XenApp- und XenDesktop-Komponenten installieren. Wenn bei der Installation Probleme auftreten, fordert Citrix Sie u. U. auf, diese Daten zur Analyse hochzuladen.

**Call Home**

Die Teilnahme an Call Home (einschließlich Always-On-Ablaufverfolgung) wird im Produktinstallationsprogramm angeboten. Sie können auch Ihre Registrierung ändern, benutzerdefinierte Uploadpläne erstellen und Pakete mit PowerShell-Cmdlets manuell hochladen.

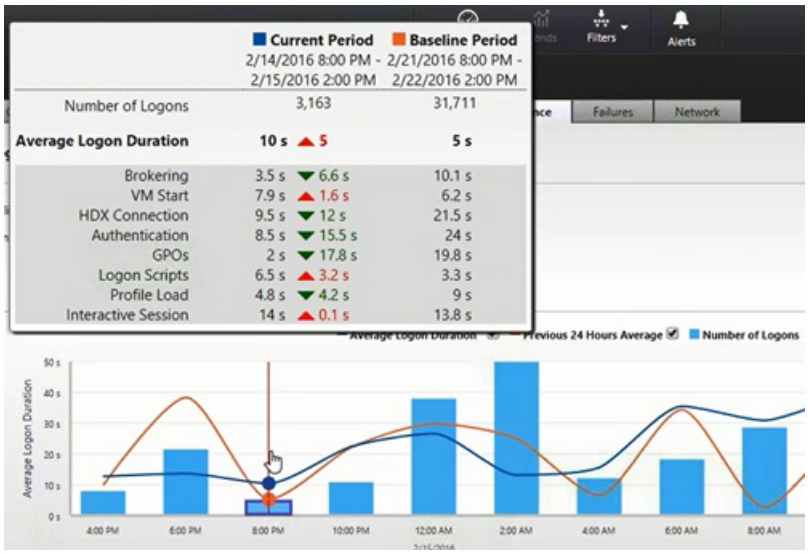
**Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)**

Die Teilnahme am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit wird beim Erstellen einer Site jetzt automatisch aktiviert. Sie brauchen keine Registrierung vorzunehmen, während der Assistent für die Siteerstellung ausgeführt wird. Sie können Ihre Teilnahme nach dem Erstellen der Site ändern.

## Director

Director enthält die folgenden neuen und erweiterten Features:

- **Verbesserungen bei der Anmeldedauer**: Das Layout der QuickInfo-Daten, die beim Auswählen eines Datenpunkts im Diagramm der Anmeldungsleistung angezeigt werden, ist nun klarer und die Daten sind einfacher zu interpretieren. Darüber hinaus wird die Anzahl der Anmeldungen durch ein Balkendiagramm dargestellt (früher durch ein Kurvendiagramm). Im Diagramm kann die Anzeige der Anzahl von Anmeldungen und des vorherigen Basiszeitraums aktiviert und deaktiviert werden. In einer neuen Tabelle wird die Anmeldedauer pro Benutzersitzung für den ausgewählten Zeitraum unter dem Anmeldungsleistungsdiagramm angezeigt. Der Administrator kann nach Benutzern suchen und die anzuzeigenden Spalten sowie die Sortierreihenfolge wählen. Weitere Informationen zu finden Sie unter Überwachen von Bereitstellungen.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Virtual Delivery Agents 7.9

Version 7.9 des VDAs für Serverbetriebssysteme und des VDAs für Desktopbetriebssysteme enthalten die folgenden Verbesserungen für das Drucken, HDX-Technologien und Plattformunterstützung:

- **Lastausgleich für Citrix universelle Druckserver (UPS)**: Administratoren können mehrere Lastausgleichsdruckserver mit zwei neuen Richtlinieneinstellungen hinzufügen: "Universelle Druckserver für den Lastausgleich" und "Außer-Betrieb-Schwellenwert für universelle Druckserver". Mit diesen Richtlinieneinstellungen können XenApp- und XenDesktop-Sitzungen auf einem VDA bei der Anmeldung nahtlos Sitzungsdrucker verschiedenen Druckservern zuordnen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Universeller Druckserver" und "Lastausgleich bei universellen Druckservern" im Artikel Pflege der Druckumgebung.
- **Heftung und Auswahl der Papierzufuhr für den universellen Citrix XPS-Druckertreiber**: Der universelle Citrix XPS-Druckertreiber unterstützt erweiterte Druckerfunktionen, wie Heftung und Auswahl der Papierzufuhr. Weitere Informationen finden Sie unter Bereitstellen von Druckern.
- **Universeller Druckserver und CEIP**: Wenn Sie den universellen Druckserver installieren, erfolgt die Registrierung für das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) automatisch. In den ersten sieben Tagen werden keine Daten gesammelt. Während dieser Zeit oder zu einem späteren Zeitpunkt können Sie die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit für UPS über eine Registrierungseinstellung deaktivieren. Weitere Informationen finden Sie unter Bereitstellen von Druckern und Citrix Insight Services.
- **Richtlinieneinstellungen für LPT- und COM-Portumleitung in Studio**: LPT- und COM-Porteinstellungen können jetzt in Studio konfiguriert werden. In VDA-Versionen 7.0 bis 7.8 konnten diese Einstellungen nur über die Registrierung konfiguriert werden. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Portumleitung" und Einstellungen der Richtlinie "Bandbreite".
- **Erweiterte HDX 3D Pro-Unterstützung für Intel CPUs mit Intel Iris Pro Graphics**: Verwenden Sie HDX 3D Pro-Grafikbeschleunigungstechnologien mit Intel CPUs der 5. und 6. Generation für Intel Iris Pro Graphics. Dieses Release umfasst Unterstützung für mehrere Monitore (maximal 3), das Ausblenden der Konsole sowie das Festlegen von benutzerdefinierter Auflösung und hoher Framerate. Die VDA-Installationsprogramme enthalten eine neue Datei, GfxDisplayTool.exe, um dieses Feature zu unterstützen. Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Desktopbetriebssysteme.
- **Unterstützung für Windows 10 im HDX 3D Pro VDA**: Dieses Release bietet Unterstützung für Windows 10 in der HDX 3D Pro-Version des VDAs für Windows-Desktopbetriebssysteme.
- **Unterstützung für sicheren Start für Remote-PC-Zugriff auf Windows 10**: Der Virtual Delivery Agent (VDA) für Desktopbetriebssysteme unterstützt sicheren Start für XenDesktop Remote-PC-Zugriff auf Windows 10 und 8.1.
- **Neue Standardeinstellung für "Videocodec zur Komprimierung verwenden"**: "Bevorzugt Videocodec verwenden" ist die neue Standardeinstellung für die Grafikrichtlinieneinstellung "Videocodec zur Komprimierung verwenden". Mit dieser Änderung wird die Verwendung des ThinWire-Kompatibilitätsmodus durch den VDA unterstützt. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Grafiken".
- **Linux VDA-Verbesserungen und Verbesserungen für Red Hat und SUSE:** Unterstützung für VC CDM und CentOS (Version 6.7, 7.2) wurde hinzugefügt, einschließlich zahlreichen Verbesserungen, um von Kunden gemeldete Probleme zu lösen. Weitere Informationen finden Sie unter Red Hat/CentOS und SUSE.
- **Generische USB-Umleitung für Massenspeichergeräte auf XenApp**: Generische USB-Umleitung (USB-Plug-n-Play) für Massenspeichergeräte wird jetzt in XenApp und XenDesktop unterstützt. XenApp-Benutzer können in einer XenApp-Sitzung Massenspeichergeräte genauso verwenden, als wäre das Speichergerät physisch angeschlossen. Um dieses Feature in XenApp zu verwenden, müssen Sie zuerst das Microsoft Security Update KB3155784 installieren. In diesem Release ist dieses Feature für XenApp standardmäßig deaktiviert und wird mit einem Registrierungsschlüssel aktiviert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zum Aktivieren von USB-Speichergeräten für die generische USB-Umleitung in XenApp müssen Sie einen Wert namens **UsbStorageEnabled** unter dem Schlüssel **HKLM\SOFTWARE\Citrix\Portica\GenericUSB** erstellen und den Wert auf **1** festlegen.

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

# StoreFront 3.6

StoreFront enthält die folgenden neuen Features:

- **Lastausgleich nicht identischer Farmen:** Beim Erstellen von äquivalenten Farmsätzen mit einer Konfiguration, die mehrere Sites umfasste, mussten in früheren Versionen von StoreFront alle Ressourcen von jedem Delivery Controller veröffentlicht werden, damit der Lastausgleich erfolgreich war. Bei der Ressourcenenumeration, bei der StoreFront eine Liste der verfügbaren Ressourcen abrief, wurde nur einer der Delivery Controller im äquivalenten Farmsatz kontaktiert. In StoreFront 3.6 können Sie Ressourcen haben, die auf allen Delivery Controllern im äquivalenten Farmsatz vorhanden sind, sowie Ressourcen, die nur von bestimmten Delivery Controllern veröffentlicht werden. Sie können nun festlegen, dass StoreFront alle Ressourcen für die Enumeration verwendet.
- **Keine Active Directory-Domäne für Einzelserverbereitstellungen erforderlich:** Möglicherweise möchten Sie Ihre Server aus verschiedenen Gründen nicht einer Active Directory-Domäne hinzufügen. Ab dieser Version ist diese Voraussetzung für Einzelserverbereitstellungen überflüssig und Sie können StoreFront auf einem Server installieren, der nicht in eine Domäne eingebunden ist.
- **StoreFront REST-API:** Wir haben eine StoreFront REST-API erstellt, die NetScaler Gateway abfragt, um die aktuelle Gateway-Konfiguration des StoreFront-Clusters zu bestimmen. Die NetScaler-Verwaltungskonsole erstellt eine Gateway-Konfigurationsdatei, die Einstellungen von StoreFront und NetScaler kombiniert. Sie können die Konfigurationsdatei mit der StoreFront-Verwaltungskonsole oder mit PowerShell in StoreFront importieren.

Weitere Informationen finden Sie in der Dokumentation zu StoreFront 3.6.

# Provisioning Services 7.9

Provisioning Services umfasst die folgenden neuen Features:

- **Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)**: CEIP sammelt anonyme Konfigurations- und Verwendungsdaten aus Provisioning Services und sendet die Daten automatisch an Citrix. Mit diesen Daten kann Citrix die Qualität, Zuverlässigkeit und Leistung von Provisioning Services verbessern.
- **BDM-Unterstützung für UEFI durch den XenDesktop-Setupassistenten**: BDM-Unterstützung für UEFI umfasst nun die Integration mit dem XenDesktop-Setupassistenten. Damit können Sie über die BDM-Startoption die UEFI-Firmware steuern. Hiermit unterstützt PVS folgende Startoptionen:
  - ISO-Image
  - USB
  - Starten von Partitionen
- **Aktualisieren einer BDM-Partition**: Mit dieser neuen Funktion von Provisioning Services 7.9 können Sie die BDM-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Partition basierend auf der Server-IP-Adresse in der Bootstrapdatei des PVS-Servers, mit dem Sie verbunden sind, aktualisieren. Für das Upgrade einer BDM-Partition gibt es drei Methoden:

- durch eine Sammlung
- durch eine Gruppe markierter Geräte
- durch ein einzelnes Gerät

Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services 7.9.

# AppDNA 7.9

AppDNA enthält die folgenden neuen Features:

- **Workflow-Verbesserungen für den Import von Anwendungen**: Verbesserungen am Workflow für den Import von Anwendungen ermöglichen Feedback zum Fortschritt der serverseitigen Verarbeitung und der Flexibilität beim Hinzufügen und Abbrechen von Importvorgängen.
- **Compliance Manager-Modul**: Mit dem Compliance Manager-Modul können Sie analysieren, ob durch Anwendungen, die Sie in der IT-Infrastruktur bereitstellen, Sicherheitsrisiken entstehen. Dieses Modul enthält einen Satz Algorithmen und Berichte, der zukünftig erweitert wird. In diesem Release ist dies ein Evaluierungsfeature und sollte nicht für Entscheidungen hinsichtlich der Bereitstellung von Anwendungen in der Produktionsumgebung verwendet werden.
- **Webclientzugriff auf Anwendungsattributformulare**: Dieses Release bietet Zugriff auf Anwendungsattributformulare über den AppDNA-Webclient. Klicken Sie im Webclient auf "Applications", markieren Sie eine Anwendung und wählen Sie "Properties".

Weitere Informationen finden Sie in der Dokumentation zu AppDNA 7.9.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Behobene Probleme

Jul 11, 2016

Die folgenden Probleme wurden seit Version 7.8 behoben:

| | |
|---|---|
| AppDNA | Provisioning Services |
| Citrix Director | StoreFront |
| Citrix Richtlinie | Universeller Druckserver |
| Citrix Studio | VDA für Desktopbetriebssystem |
| Controller | VDA für Serverbetriebssystem |
| HDX MediaStream Flash-Umleitung | Virtual Desktop-Komponenten – Sonstiges |

## AppDNA

### Citrix Director

- Beim Exportieren einer großen Datenmenge im PDF-Format kann die CPU- und Arbeitsspeicherauslastung 100 % betragen. Daraufhin wird die folgende Fehlermeldung angezeigt:

  Aktion fehlgeschlagen. Datenquelle reagiert nicht oder hat einen Fehler gemeldet. In den Ereignisprotokollen finden Sie weitere Informationen.

  Dieser Fix führt ein konfigurierbares Limit für den PDF-Export ein, sodass wenigstens ein Teil des Berichts abgerufen werden kann.

  Nach der Installation dieses Fixes müssen Sie die Datei web.config im Ordner wwwroot\Director wie folgt konfigurieren:

  Fügen Sie die folgende Zeile im Abschnitt "appSettings" hinzu:

  Das Limit hängt von der Leistungsfähigkeit des Servers ab, z. B. von der Speichergröße, wobei der Wert die Anzahl der Zeilen im PDF-Bericht angibt.

  [#LC4108]

- Das Exportieren von Berichten in einem beliebigen Dateiformat schlägt möglicherweise fehl und die folgende Fehlermeldung wird angezeigt:

  Aktion fehlgeschlagen. Unerwarteter Serverfehler. In den Ereignisprotokollen finden Sie weitere Informationen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4281]

- Wenn ein XenApp-Server zwei IP-Adressen hat und der DNS-Server die erste IP-Adresse nicht auflösen kann, schlagen die Anmeldeversuche eines Administrators an Citrix Director u. U. fehl und die folgende Fehlermeldung wird angezeigt:

  Das System ist zurzeit nicht verfügbar. Versuchen Sie es später noch einmal oder wenden Sie sich an den Administrator.

  [#LC4411]

- Wenn Sie versuchen, eine große Menge der Daten im CSV-Format zu exportieren, kann ein Timeout auftreten und der Export schlägt möglicherweise mit der folgenden Fehlermeldung fehl:

  Aktion fehlgeschlagen. Datenquelle reagiert nicht oder hat einen Fehler gemeldet. Weitere Informationen finden Sie in den Serverereignisprotokollen von Director.

  Mit diesem Fix konfigurieren Sie den Timeoutwert für den Export von Daten.

  Nach der Installation des Fixes müssen Sie die Datei web.config im Ordner wwwroot\Director wie folgt konfigurieren:

  Fügen Sie die folgende Zeile im Abschnitt "appSettings" hinzu:
  , wobei der Wert das Timeout in Sekunden angibt.

  [#LC4467]

- Wenn Sie einen Benutzer auswählen, um die Sitzungsdetails des Benutzers anzuzeigen, wird möglicherweise der Benutzername oben links als "NULL" angezeigt.

  [#LC4589]

- Enthält der NetBIOS-Domänenname ein kaufmännisches Und-Zeichen (&), schlägt das Spiegeln von der Citrix Director-Konsole aus möglicherweise fehl. Dieses Problem tritt auf, weil das &-Zeichen in XML ein reserviertes Zeichen ist und zu einem Fehler beim Parsen für die aktuelle Anmeldung führen kann.

  [#LC4633]

- Citrix Director mit integrierter Windows-Authentifizierung (WIA) funktioniert eventuell nicht mit eingeschränkter Kerberos-Delegierung.

  [#LC5196]

### Citrix Richtlinie

- Citrix Director-Administratoren können Citrix Richtlinien u. U. nicht in den Sitzungsdetails anzeigen.

  [#LC3941]

- Beim Hinzufügen mehrerer Sitzungsdrucker zu einer Gruppe von Benutzergeräten im Fenster "Druckerzuordnungen" wird das Fenster nicht erweitert und die Bildlaufleiste wird nicht angezeigt. Daher kann der Versuch, mehrere Sitzungsdrucker einer Gruppe von Benutzergeräten zuzuordnen, fehlschlagen.

  [#LC4658]

- Citrix Director-Administratoren können Citrix Richtlinien u. U. nicht in den Sitzungsdetails anzeigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4956]

### Citrix Studio

- Wenn Sie mit den Maschinenerstellungsdiensten VDAs für Serverbetriebssystemmaschinen katalogisieren und es ist nicht ausreichend persönlicher vDisk-Speicher vorhanden, wird die Eigenschaft "CleanOnBoot" des Katalogs u. U. fälschlicherweise auf "False" festgelegt. Der Katalog wird dann möglicherweise nicht aktualisiert.

  [#LC2959]

- Das Erstellen mehrerer Anwendungen in mehreren Ordnern unter Bereitstellungsgruppen in Citrix Studio kann zu einer umfangreichen Ordnerstruktur führen. Wenn Sie Citrix Studio das erste Mal öffnen und auf Ordner oder Anwendungen klicken, werden die Ordner oder Anwendungen möglicherweise gezogen und nicht ausgewählt. Dadurch wird das ausgewählte Objekt verschoben und die Ordner- bzw. Anwendungsstruktur verändert.

  [#LC3705]

- Das Öffnen von Citrix Studio durch Benutzer, die keine Mitglieder der Benutzergruppe der Datenbankadministratoren sind, kann zu Berechtigungsfehlern auf dem SQL Server führen.

  [#LC4127]

- Das Provisioning weiterer Ressourcen für ein mandantenfähiges Angebot in App Orchestration 2.6 kann fehlschlagen, wenn das Angebot bereits zwei oder mehr Mandanten enthält.

  [#LC4170]

- Wenn ein Delivery Controller offline geht oder aus anderen Gründen nicht verfügbar ist, wird Citrix Studio möglicherweise langsam ausgeführt.

  [#LC4481]

- Das Hinzufügen von Maschinen zu einem Maschinenkatalog in Citrix Studio kann fehlschlagen und zur Anzeige einer Fehlermeldung führen. Das Problem tritt nicht auf, wenn Sie Maschinen mit dem XenDesktop-Setupassistenten hinzufügen.

  [#LC5030]

### Controller

- Der geplante Neustart eines VDAs für Serverbetriebssysteme, der mit einem VMware Vsphere Hypervisor verbunden ist, kann dazu führen, dass der Server heruntergefahren wird und ausgeschaltet bleibt.

  - Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
    Name: ShutdownTimeoutRecovery
    Typ: DWORD
    Wert: 1

  - Um die Implementierung des Fixes aufzuheben, legen Sie folgenden Registrierungsschlüssel fest:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule
    Name: ShutdownTimeoutRecovery


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Typ: DWORD
Wert: 0

Nachdem Sie den Wert festgelegt haben, müssen Sie den Brokerdienst neu starten.

[#LC3807]

- Das Öffnen von Citrix Studio durch Benutzer, die keine Mitglieder der Benutzergruppe der Datenbankadministratoren sind, kann zu Berechtigungsfehlern auf dem SQL Server führen.

  [#LC4127]

- Wenn die Einstellung "SupportMultipleForest" auf dem Controller aktiviert ist, um NTLM-Authentifizierung zu ermöglichen, schließt der Linux-VDA möglicherweise den Registrierungsvorgang nicht ab, weil sein Dienstprinzipalname (Service Principal Name, SPN) u. U. nicht im EndpointReference der Windows Communication Foundation (WCF) festgelegt ist.

  [#LC4235]

- Wenn ein Delivery Controller offline geht oder aus anderen Gründen nicht verfügbar ist, wird Citrix Studio möglicherweise langsam ausgeführt.

  [#LC4481]

- Die WaitForTask-Antwort verursacht die Ausnahme VimApi.MissingProperty, die das Aktualisieren von Maschinenkatalogen nicht zulässt.

  [#LC4573]

- Wenn Sie den PowerShell-Befehl "Get-LogSummary" für einen Datumsbereich ausführen, der einen Wechsel zwischen Standardzeit und Sommerzeit einschließt, wird die folgende Fehlermeldung angezeigt:

  "Ein Element mit dem gleichen Schlüssel wurde bereits hinzugefügt."

  Das Problem tritt auf, wenn durch die Sommerzeit zusätzliche Werte für das lokale Datum oder die lokale Zeit eingeführt werden, sodass Datum und Zeit nicht mehr eindeutig sind. Dadurch werden doppelte Einträge in der Hashzuordnung erstellt und eine Ausnahme tritt auf.

  Dieser Fix führt eine Meldung ein, die Benutzern rät, eine Zeitspanne, die den Beginn oder das Ende der Sommerzeit einschließt, am Zeitpunkt der Zeitumstellung aufzuteilen.

  [#LC4612]

- Das Aktualisieren von Maschinenkatalogen in Amazon Web Services (AWS)-Umgebungen kann gelegentlich fehlschlagen. Um den Fix zu aktivieren, führen Sie den Befehl "Set-ProvServiceConfigurationData –Name ImageManagementPrep_DoImagePreparation –Value $false" aus, damit die Imagevorbereitungsphase während der Aktualisierung der Maschinenkataloge übersprungen wird.

  [#LC4709]

- Controller verlieren manchmal die Verbindung mit der Datenbank, wenn eine große Anzahl von Apps und VDA-Prozessen ausgeführt werden. In diesem Fall bleiben VDAs im Initialisierungszustand und Anwendungen sind nicht verfügbar.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4848]

- Das Hinzufügen von Maschinen zu einem Maschinenkatalog in Citrix Studio kann fehlschlagen und zur Anzeige einer Fehlermeldung führen. Das Problem tritt nicht auf, wenn Sie Maschinen mit dem XenDesktop-Setupassistenten hinzufügen.

  [#LC5030]

- Dieser Fix behebt ein Problem, das das Provisioning mit Maschinenerstellungsdienste in Amazon Web Services verhindert, wenn der Controller von Amazons öffentlichen API-Endpunkten durch einen Webproxy isoliert ist.

  [#LC5109]

### HDX MediaStream Flash-Umleitung

- Wenn HDX MediaStream für Flash aktiviert ist, kann das Öffnen und Schließen von mehreren Registerkarten mit Flash-Inhalten in Internet Explorer dazu führen, dass Internet Explorer unerwartet beendet wird.

  [#LA3065]

- Wenn HDX MediaStream für Flash aktiviert ist, führt das Öffnen und Schließen von mehreren Registerkarten in Internet Explorer u. U. dazu, dass Internet Explorer unerwartet geschlossen wird.

  [#LC1141]

- Wenn HDX MediaStream Flash-Umleitung aktiviert ist, wird Microsoft Internet Explorer möglicherweise unerwartet geschlossen, wenn pseudoserverinproc2.dll ausgeführt wird.

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

  - *Windows-32-Bit-Systeme:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Name: AllowCOMObjectTrack
    Typ: DWORD
    Wert: 0

  - *Windows-64-Bit-Systeme:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
    Name: AllowCOMObjectTrack
    Typ: DWORD
    Wert: 0

  [#LC1885]

- Wenn HDX MediaStream Flash-Umleitung aktiviert ist und Sie Websites durchsuchen, schlägt das Flash-Umleitungsfeature fehl, wenn der Registrierungswert HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs nur auf "mfaphook.dll" oder "mfaphook64.dll" festgelegt ist statt auf den vollständigen Pfad für "mfaphook.dll" oder "mfaphook64.dll."

  [#LC4388]


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provisioning Services 7.9

StoreFront 3.6

Universeller Druckserver

| Client | Server |
| --- | --- |

## Einstellungen

- Beim Drucken auf dem universellen Druckserver schlägt die NextGen-Anwendung gelegentlich fehl.

  [#LC4246]

## Server

- Das Batchdrucken mit der Microsoft GDI Print API kann fehlschlagen, sodass die letzte Seite nicht gedruckt und die folgende Fehlermeldung angezeigt wird:

  "Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check Printer"

  [#LC3920]

- Dieser Fix bietet Unterstützung für das Citrix UPS Print Driver Certification Tool für Universal Print Server 7.6.300. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX142119.

  [#LC4265]

VDA für Desktopbetriebssystem

| | Smartcards |
| --- | --- |
| HDX MediaStream Windows Media-Umleitung | Systemausnahmen |
| Drucken | Benutzererfahrung |
| Sitzung/Verbindung | Benutzeroberfläche |

**HDX MediaStream Windows Media-Umleitung**

- Wenn Sie eine AVI-Datei mit Windows Media Player in einer ICA-Sitzung (oder einer veröffentlichten Desktopsitzung) wiedergeben und dann mit der Wiedergabe einer anderen AVI-Datei beginnen, ohne die erste anzuhalten, werden die Videoframes möglicherweise nicht richtig an das Benutzergerät weitergeleitet. Daher ist die CPU-Auslastung des Prozesses mmvdhost.exe u. U. höher als normalerweise und das Video wird nicht richtig auf dem Benutzergerät wiedergegeben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4260]

- Wenn HDX MediaStream Windows Media-Umleitung aktiviert ist, werden bestimmte Drittanbieter-Player u. U. unerwartet beendet, während Dateien auf einem VDA wiedergegeben werden, der auf Windows 10 ausgeführt wird.

  [#LC5110]

**Drucken**

- Der Citrix Druckspoolerdienst wird möglicherweise unerwartet beendet.

  [#LC4180]

- Die Richtlinie "Clientdrucker automatisch erstellen" legt Standarddrucker in einer veröffentlichten Anwendung u. U. nicht richtig fest und stattdessen wird Microsoft XPS Document Writer als Standarddrucker festgelegt.

  [#LC4696]

**Sitzung/Verbindung**

- Die Richtlinie "Regeln für die Client-USB-Geräteumleitung" wird u. U. nicht angewendet. Das Problem tritt auf, wenn die Anzahl der vom Benutzer eingegebenen Zeichen in der Richtlinie 1002 überschreitet.

  [#LC1144]

- Wenn auf einem Endpunkt mehrere Webcams und Videoaufnahmegeräte installiert sind, wird nur eins der Geräte der Sitzung zugeordnet. Außerdem wird das Gerät als "Citrix HDX Web Camera" zugeordnet, sodass nicht identifiziert werden kann, um welches Gerät es sich handelt.

  [#LC1919]

- Bestimmte veröffentlichte Anwendungen von Dritten starten auf XenApp-Servern möglicherweise nicht. Daher kann der Prozess wfshell.exe unerwartet geschlossen werden. Wenn dieses Problem auftritt, ist nicht ersichtlich, dass die Sitzung gestartet wird, und es wird keine Fehlermeldungen auf dem Benutzergerät angezeigt.

  [#LC3766]

- Nachdem die Thomson Reuters Eikon-Symbolleiste in einer Sitzung mit mehreren Monitoren abgedockt wurde, wird der Platz, den die Symbolleiste einnahm, nicht von der Sitzung eingenommen.

  Bei Monitorkonfigurationen, in denen der primäre Monitor nicht oben links in der Anordnung ist, müssen Sie auch den Fix #LC1599 installieren, der in Receiver für Windows 4.4 und höher enthalten ist.

  [#LC3773]

- Wenn auf dem Sitzungshost die App-V-Konfigurationseinstellung "EnablePublishingRefreshUI" und darüber hinaus "Sitzungsfortbestehen" aktiviert ist, kann das Schließen einer Anwendung auf einem iOS-Gerät zu einem schwarzen Fenster führen, das auf dem Bildschirm des Geräts bleibt.

  [#LC3800]

- Wenn Sie während einer ICA-Sitzung einen Remote-PC ausschalten oder einen Neustart erzwingen, sind u. U. alle Audiotreiber deaktiviert, wenn der Neustart des Remote-PCs abgeschlossen ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4071]

- Nach der Installation des Hotfix ICAWS760WX64032 und dem Aktivieren von SSL schlagen Wiederverbindungsversuche mit einem VDA gelegentlich fehl. Das Problem tritt auf, wenn der Citrix ICA-Dienst unerwartet beendet wird oder aufgrund eines SSL-Listener-Fehlers nicht mehr reagiert.

  [#LC4438]

- Nach einer Netzwerkunterbrechung zwischen einem VDA und Citrix Receiver können Sie keine AVI-Dateien auf dem Windows Media Player wiedergeben.

  [#LC4670]

- Nach einer Netzwerkunterbrechung schlagen Wiederverbindungsversuche mit einem VDA möglicherweise fehl. Das Problem tritt nach einem Upgrade des VDAs auf Version 7.8 auf.

  [#LC5040]

- Dieser Fix behebt ein Problem, bei dem der clientseitige Inhaltsabruf für Anwendungen, die auf DirectShow basieren, nicht funktioniert, sodass Videos nicht wiedergegeben werden können.

  [#LC5098]

**Smartcards**

- In Microsoft Internet Explorer ist die Benutzeroberfläche für Smartcard-Anmeldungen für bestimmte Websites u. U. gelegentlich nicht verfügbar.

  [#LC3988]

- Auf VDAs Version 7.6.300 und höher, die auf Windows 10 Build 10586 und höher ausgeführt werden, wird die Anmeldeoption nicht angezeigt. Daher sind Smartcard-Anmeldungen nicht möglich.

  [#LC4778]

**Systemausnahmen**

- Im Betriebssystem kommt es zu einem Fehler mit ctxad.sys und ein Bluescreen mit Bugcheckcode 0xD1 wird angezeigt.

  [#LC4007]

- Wenn Sie auf Windows Media Player eine AVI-Datei mehrfach wiedergeben, steigt der Speicherverbrauch des Prozesses wfica32.exe u. U. immer weiter an, bis der Prozess unerwartet geschlossen wird.

  [#LC4335]

- Wenn der Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses definiert ist, können Neustarts des VDAs und das Starten eines veröffentlichten Desktops zu einem Bluescreen führen.

  [#LC4597]

- Ein veröffentlichter Anwendungsprozess wird möglicherweise mit der Ausnahme "c000041d" auf MobileDesktopHook64.dll unerwartet beendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC4821]

**Benutzererfahrung**

- Wenn Sie von einem touchoptimierten veröffentlichten Desktop zu einem regulären veröffentlichten Desktop wechseln, zeigt die Schaltfläche "Start" folgendes Verhalten:
  - Sie wird nicht hervorgehoben, wenn Sie mit dem Mauszeiger darauf zeigen.
  - Sie ruft den lokalen Desktop statt des veröffentlichten Desktops auf.

  [#LC3466]

**Benutzeroberfläche**

- Nach dem Veröffentlichen von Anwendungen im Seamless-Modus wird u. U. das generische Citrix Receiver-Symbol statt des Symbols für die veröffentlichte Anwendung in der Taskleiste angezeigt.

  [#LC4757]

## VDA für Serverbetriebssystem

| | |
|---|---|
| HDX MediaStream Windows Media-Umleitung | Smartcards |
| Drucken | Systemausnahmen |
| Server-/Siteverwaltung | Benutzererfahrung |
| Sitzung/Verbindung | Benutzeroberfläche |

**HDX MediaStream Windows Media-Umleitung**

- Wenn Sie eine AVI-Datei mit Windows Media Player in einer ICA-Sitzung (oder einer veröffentlichten Desktopsitzung) wiedergeben und dann mit der Wiedergabe einer anderen AVI-Datei beginnen, ohne die erste anzuhalten, werden die Videoframes möglicherweise nicht richtig an das Benutzergerät weitergeleitet. Daher ist die CPU-Auslastung des Prozesses mmvdhost.exe u. U. höher als normalerweise und das Video wird nicht richtig auf dem Benutzergerät wiedergegeben.

  [#LC4260]

- Wenn HDX MediaStream Windows Media-Umleitung aktiviert ist, werden bestimmte Drittanbieter-Player u. U. unerwartet beendet, während Dateien auf einem VDA wiedergegeben werden, der auf Windows 10 ausgeführt wird.

  [#LC5110]

**Drucken**

- Der Citrix Druckspoolerdienst wird möglicherweise unerwartet beendet.

  [#LC4180]


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Automatisch erstellte Drucker sind möglicherweise nicht in einer veröffentlichten Anwendung verfügbar, wenn Legacy-Druckernamen aktiviert sind und mehrere Sitzungen für denselben Benutzer auf einem Server hergestellt wurden.

  [#LC4517]

- Die Druckerumleitung kann gelegentlich fehlschlagen.

  [#LC4584]

- Die Richtlinie "Clientdrucker automatisch erstellen" legt Standarddrucker in einer veröffentlichten Anwendung u. U. nicht richtig fest und stattdessen wird Microsoft XPS Document Writer als Standarddrucker festgelegt.

  [#LC4696]

**Server-/Siteverwaltung**

- Wenn Benutzer zwischen Sitzungen wechseln, die in einem Netzwerk in verschiedenen Subnetzen sind, enthält die Druckerliste Drucker beider Subnetze statt der Drucker des Subnetzes, bei dem Benutzer zurzeit angemeldet sind.

  [#LC2308]

- Mehrere gleichzeitige Versuche, eine Remote Desktop (RDP)-Verbindung mit einem VDA von unterschiedlichen Benutzergeräten aus zu erstellen, können dazu führen, dass die Registrierung des VDAs aufgehoben wird.

  [#LC4014]

**Sitzung/Verbindung**

- Wenn die Richtlinien für die Clientaudioumleitung oder die Windows Media-Umleitung deaktiviert sind, zeigt das Symbol für die Lautstärkesteuerung (Lautsprecher) im Infobereich einer veröffentlichten Desktopsitzung möglicherweise den falschen Audiozustand an.

  [#LC2538]

- Standardmäßig werden die Windows-Verknüpfungen für den Schnellzugriff auf "Desktop" und "Downloads" bei der Anmeldung unter %userprofile%\Links neu erstellt, wenn Sie sie zuvor manuell gelöscht haben. Dieses Verhalten ist nicht für alle Szenarios erwünscht. Dieser Fix führt Unterstützung für den folgenden Registrierungsschlüssel ein. Wenn er auf 0 (Null) festgelegt ist, wird die automatische Neuerstellung der zwei Verknüpfungen verhindert:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell
  Name: CreateShortcutLinks
  Typ: REG_DWORD
  Wert: 0

  [#LC3274]

- Dieser Fix behebt ein Problem, das zur gelegentlichen Beschädigung von Dateien führt, die auf zugeordnete Clientlaufwerke geschrieben werden.

  [#LC3684]

- Bestimmte veröffentlichte Anwendungen von Dritten starten auf XenApp-Servern möglicherweise nicht. Daher kann der Prozess wfshell.exe unerwartet geschlossen werden. Wenn dieses Problem auftritt, ist nicht ersichtlich, dass die Sitzung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

gestartet wird und es wird keine Fehlermeldungen auf dem Benutzergerät angezeigt.

[#LC3766]

- Nachdem die Thomson Reuters Eikon-Symbolleiste in einer Sitzung mit mehreren Monitoren abgedockt wurde, wird der Platz, den die Symbolleiste einnahm, nicht von der Sitzung eingenommen.

  Bei Monitorkonfigurationen, in denen der primäre Monitor nicht oben links in der Anordnung ist, müssen Sie auch den Fix #LC1599 installieren, der in Receiver für Windows 4.4 und höher enthalten ist.

  [#LC3773]

- Ist Excelhook aktiviert und Sie minimieren mehrere geöffnete Excel-Arbeitsmappen, können Sie möglicherweise keine der Arbeitsmappen in den Vordergrund bringen.

  [#LC3799]

- Wenn auf dem Sitzungshost die App-V-Konfigurationseinstellung "EnablePublishingRefreshUI" und darüber hinaus "Sitzungsfortbestehen" aktiviert ist, kann das Schließen einer Anwendung auf einem iOS-Gerät zu einem schwarzen Fenster führen, das auf dem Bildschirm des Geräts bleibt.

  [#LC3800]

- Selbst bei aktivierter Richtlinie für die Clientaudioumleitung können Audiodateien (.wav) möglicherweise nicht wiedergegeben werden. Das Problem tritt in Sitzungen auf, in denen die Sitzungs-ID erneut verwendet wird und die Richtlinie für die Clientaudioumleitung für die vorherige Sitzung deaktiviert wurde.

  [#LC3882]

- Bei Systemen mit Fix #LC2702 (im Hotfix Rollup Pack 6 enthalten) werden Anwendungen u. U. nicht auf zugeordneten Clientlaufwerken gespeichert und stattdessen werden beschädigte Dateien generiert.

  [#LC3976]

- In veröffentlichten Instanzen von Microsoft Internet Explorer kann das Herunterladen einer Datei von einer Website und das Speichern auf einem zugeordneten Clientlaufwerk ("Speichern unter...") fehlschlagen.

  [#LC4300]

- Aufgrund der Datei icaendpoint.dll wird der Windows Audiodienst möglicherweise unerwartet beendet.

  [#LC4356]

- Wenn ein anderer Prozess die gleiche Sperre wie picadm.sys hat, können sich Benutzer nicht von der Sitzung abmelden und die Sitzung bleibt im getrennten Zustand.

  [#LC4415]

- Bei Systemen mit Fix #LC0615 können Sitzungsabmeldungen länger als erwartet dauern.

  [#LC4674]

- Das Starten eines Prozesses mit WinDbg.exe schlägt möglicherweise fehl, wenn Streaming Profiler oder das Offline-Plug-In installiert sind. Dieses Problem tritt auf, weil RadeAPHook einen Hook für die Einstellung für


© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*> und HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*> aufruft.

Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

- *Bei 32-Bit-Windows:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
  Name: EnableReadImageFileExecOptionsExclusionList
  Typ: Reg_SZ
  Wert: <*Durch Kommas getrennte Liste (ohne Leerstellen) der ausführbaren Dateien, die vom Hooking in Bezug auf die Einstellung "Image File Execution Options" ausgenommen werden. Beispiel: windbg.exe,application_1.exe.*>

- *Bei 64-Bit-Windows für 32-Bit-Anwendungen:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  Name: EnableReadImageFileExecOptionsExclusionList
  Typ: Reg_SZ
  Wert: <*Durch Kommas getrennte Liste (ohne Leerstellen) der ausführbaren Dateien, die vom Hooking in Bezug auf die Einstellung "Image File Execution Options" ausgenommen werden. Beispiel: windbg.exe,application_1.exe.*>

[#LC4750]

- Dieser Fix behebt ein Problem, bei dem der clientseitige Inhaltsabruf für Anwendungen nicht funktioniert, die auf DirectShow basieren, sodass Videos nicht wiedergegeben werden können.

  [#LC5098]

**Smartcards**

- In Microsoft Internet Explorer ist die Benutzeroberfläche für Smartcard-Anmeldungen für bestimmte Websites u. U. gelegentlich nicht verfügbar.

  [#LC3988]

- Auf VDAs Version 7.6.300 und höher, die auf Windows 10 Build 10586 und höher ausgeführt werden, wird die Anmeldeoption nicht angezeigt. Daher sind Smartcard-Anmeldungen nicht möglich.

  [#LC4778]

**Systemausnahmen**

- Wenn Sie auf Windows Media Player eine AVI-Datei mehrfach wiedergeben, steigt der Speicherverbrauch des Prozesses wfica32.exe u. U. immer weiter an, bis der Prozess unerwartet geschlossen wird.

  [#LC4335]

- Wenn der Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses definiert ist, können Neustarts des VDAs und das Starten eines veröffentlichten Desktops zu einem Bluescreen führen.

  [#LC4597]

- Ein veröffentlichter Anwendungsprozess wird möglicherweise mit der Ausnahme "c000041d" auf

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

MobileDesktopHook64.dll unerwartet beendet.

[#LC4821]

**Benutzererfahrung**

- Wenn Sie von einem touchoptimierten veröffentlichten Desktop zu einem regulären veröffentlichten Desktop wechseln, zeigt die Schaltfläche "Start" folgendes Verhalten:

  - Sie wird nicht markiert, wenn Sie mit dem Mauszeiger darauf zeigen.
  - Sie ruft den lokalen Desktop statt des veröffentlichten Desktops auf.

  [#LC3466]

- Wenn Sie ein Microsoft Excel-Fenster in einer Seamless-Sitzung mit zwei Bildschirmen verschieben, tritt u. U. beim Aktualisieren der Darstellung des Fensters am neuen Ort eine Verzögerung auf.

  [#LC4441]

**Benutzeroberfläche**

- Nach dem Veröffentlichen von Anwendungen im Seamless-Modus wird u. U. das generische Citrix Receiver-Symbol statt des Symbols für die veröffentlichte Anwendung in der Taskleiste angezeigt.

  [#LC4757]

# Virtual Desktop-Komponenten – Sonstiges

- Anwendungen mit App-V-Integration werden u. U. nicht gestartet, wenn das konfigurierte Arbeitsverzeichnis nicht vorhanden ist.

  [#LC4839]


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bekannte Probleme

Aug 17, 2016

Der folgende Warnhinweis gilt für alle Workarounds, bei denen ein Registrierungseintrag geändert werden muss:

> **Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

# XenApp und XenDesktop

Bei Release 7.9 von XenApp und XenDesktop gibt es folgende Probleme:

- Wird ein USB-Massenspeichergerät am Endpunkt verwendet und die USB-Umleitungsrichtlinie ist aktiviert, wird möglicherweise der Fehler "Gerät in Verwendung" gemeldet, wenn versucht wird, das Gerät auszuwerfen.
  - Installieren Sie in einer Remote-PC-Zugriffsumgebung den VDA über die Befehlszeile neu. Dadurch wird verhindert, dass der Fehler erneut auftritt.
  - In anderen Umgebungen versuchen Sie einen der folgenden Workarounds:
    - Verwenden Sie anstelle der generischen Umleitung die Umleitung über optimierte virtuelle Kanäle. Dadurch können USB-Geräte über die Clientmaschine ausgeworfen werden. Weitere Informationen finden Sie unter CTX137939 und im Artikel Client-USB-Geräteumleitung.
    - Deaktivieren Sie über Windows auf dem USB-Gerät den Schreibcache und optimieren Sie das Gerät für schnelles Entfernen. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation. [#628442]
- Wenn auf dem Server, auf dem der Delivery Controller installiert wird, bereits SQL Server Express 2008 R2 ohne Service Packs installiert ist, tritt in Studio bei der Siteerstellung ein Fehler auf. (Dieses Problem tritt selbst dann auf, wenn Sie diese Datenbank nicht als Site- Protokollierungs- oder Überwachungsdatenbank verwenden.) Zur Vermeidung des Problems führen Sie vor der Installation des Controllers einen der folgenden Schritte durch: Installieren Sie ein Service Pack für SQL Server Express 2008 R2 oder deinstallieren Sie SQL Server Express 2008 R2. [#632483]
- Wenn eine für die AppDisk-Erstellung verwendete Maschine nicht die aktuelle Liste der Delivery Controller ("ListOfDDCs") hat, werden Controlleranforderungen zum Erstellen einer AppDisk möglicherweise nicht bestätigt und schlagen fehl. Das normale Feature für automatische Updates funktioniert bei diesen Maschinen nicht. Sie müssen die Liste "ListOfDDCs" über Richtlinieneinstellungen oder die Registrierung manuell aktualisieren (siehe Artikel "Delivery Controller"). [#633341]
- Wenn Sie beim Erstellen einer Site die SQL Server Express-Datenbank zur Verwendung als Sitedatenbank installieren (dies ist die Standardeinstellung), wird nach der Installation der Datenbanksoftware ein Neustart ausgeführt. Der Neustart wird nicht ausgeführt, wenn Sie die SQL Server Express-Software zur Verwendung als Sitedatenbank nicht installieren. [#634316]
- Die VDA-Installation unter einem Windows Server-Betriebssystem kann fehlschlagen, wenn auf der Maschine nicht die neuesten Windows-Updates installiert sind. (Für Windows Server 2008 R2 muss KB2685811 installiert sein, die neueren unterstützten Betriebssysteme enthalten diese Updates bereits.) [#635456]
- Wenn Sie keine Berechtigung für die Verwendung des Citrix Lizenzservers haben und im Studio-Navigationsbereich "Konfiguration > Lizenzierung" auswählen und dann im Aktionsbereich auf **Anmelden** klicken, stürzt das Studio-Snap-In ab. Starten Sie Studio neu, es wiederherzustellen. (Sie können den Lizenzserver direkt über die License Administration Console verwalten). [#640925]
- Wenn Sie App-V-Server in Studio konfiguriert haben, stürzt die Microsoft Management Console (MMC) u. U. ab, wenn Sie Studio schließen. [#652949]
- Wenn Sie lokalen Speicher für das Betriebssystem und Writebackcache verwenden, stellen Sie sicher, dass für beides derselbe Speicher verwendet wird. Wenn die Speicherliste für den Writebackcache Speicher enthält, der nicht für den Betriebssystemspeicher verfügbar ist, wird während der Katalogerstellung u. U. der Fehler "Unable to find file [Datastore]" angezeigt. [#637430]
- Beim Erstellen von AppDisks mit einer Windows 10-Maschine wird der Versiegelungsvorgang möglicherweise nicht erfolgreich beendet. Als Workaround löschen Sie die AppDisk (mit dem PowerShell-Cmdlet Remove-AppLibAppDisk) und erstellen Sie dann die AppDisk noch einmal. [#633998]
- Das Upgrade von StoreFront mit dem Produktinstallationsprogramm für XenApp und XenDesktop wird u. U. nicht erfolgreich abgeschlossen. Sie verhindern das erneute Auftreten dieses Problems, indem Sie den StoreFront-Server neu starten, damit eventuell vorhandene Dateisperren entfernt werden. Führen Sie dann das Installationsprogramm aus, ohne eine Citrix Verwaltungskonsole oder PowerShell-Sitzung zu öffnen. [#641242]
- Nach einem Upgrade von Version 7.5 (oder von 7.6, sofern diese Version als Upgrade von 7.5 installiert wurde) wird Studio oder das High-Level-SDK möglicherweise nicht gestartet. Workaround: Führen Sie eine Reparaturinstallation des Studio-MSI-Pakets ([XDInstallerRoot]\x64\DesktopStudio\DesktopStudio_x64.msi) oder des High-Level-SDK-MSI-Pakets ([XDInstallerRoot]\x64\Citrix Desktop Delivery Controller\XDPoshSnapin.msi) durch. [#617897]
- In großen Sites können durch veraltete SQL-Statistiken und fragmentierte Indizes Leistungsprobleme in Studio und Director verursacht werden. Zur Problemvermeidung sollte der Datenbankadministrator außerhalb der Stoßzeiten eine SQL Server-Wartung durchführen, bei der die Indizes und Statistiken für die Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank neu erstellt werden. Weitere Informationen finden Sie in der Dokumentation zu


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wartungsplänen für Ihre SQL Server-Version. [#641889]

- Anmeldedauerwerte für eine gelöschte Bereitstellungsgruppe werden im Diagramm als "Nicht zutreffend" angezeigt und die Zeile wird in der Tabelle nicht angezeigt, wenn die Bereitstellungsgruppe gelöscht ist und Sie die Bereitstellungsgruppe ausgewählt haben. [#615106]
- Wenn Sie unter **Trends** > **Kapazitätsverwaltung**> **Nutzung gehosteter Anwendungen** nach Nutzungsdauer oder eigenständigen Benutzern sortieren, tritt ein Fehler auf. Starten Sie als Workaround Director neu. [#640508]
- Das Verwenden des Mausrads zum Klicken in einer Framehawk-Sitzung führt u. U. zu unerwarteten Ergebnissen. [#625408]
- Wenn Sie einen HDX 3D Pro VDA in einer Remote-PC-Zugriff-Bereitstellung trennen, in der Intel CPUs mit Intel Iris Pro Graphics verwendet werden, wird die Helligkeit des Konsolenmonitors reduziert. Dies ist ein Drittanbieterproblem. Als Workaround starten Sie das Remote-PC-Zugriff-Gerät neu, um die Helligkeit des Monitors wiederherzustellen. [#633101]
- In einer Remote-PC-Zugriff-Bereitstellung unter Windows 10 (nur 32 Bit) mit einem HDX 3D Pro VDA startet das Remote-PC-Zugriff-Gerät nicht mehr, nachdem ein Intel-Treiber der Version 20.19.15.9999 installiert wurde. Dies ist ein Drittanbieterproblem. Verwenden Sie als Workaround Treiber von Windows Update. [#637294] **Hinweis**: Für Remote-PC-Zugriff wird der VDA normalerweise mit der Standard-VDA-Option konfiguriert. Weitere Informationen zum Konfigurieren des VDAs im Standardmodus oder im HDX 3D Pro-Modus finden Sie unter Vorbereiten der Installation.
- Die Installation von XenApp und XenDesktop wird nach der Installation von .NET 4.5.2 nicht fortgesetzt. Dieses Problem tritt unter Windows Server 2008 R2 auf. Als Workaround installieren Sie .NET 4.5.2 manuell und wiederholen dann die Installation. [633721]
- Wenn während einer Remote-PC-Sitzung mehrere Eingabegeräte über USB angeschlossen sind (mit Ausnahme von Maus und Tastatur), und Sie trennen ein Gerät, z. B. ein Touchpad, und schließen es wieder an, nachdem Sie die Sitzung getrennt und wiederverbunden haben, dann bleibt das USB-Eingabegerät deaktiviert. Als Workaround müssen Sie das Eingabegerät manuell aktivieren. [#638766]
- Wenn der ThinWire-Kompatibilitätsmodus aktiviert ist und Sie ziehen ein Video über mehrere Monitore, treten u. U. Fehler bei der Grafikanzeige auf (in Sitzungen mit mindestens drei Monitoren oder mehr). [#640437]
- Wenn ein Benutzer einen Surface Pro herunterfährt und dann wieder neu startet, funktionieren HDX-Verbindungen über Remote-PC-Zugriff möglicherweise nicht. Als Workaround starten Sie die Maschine neu. [#634830]
- Beim Herstellen einer Verbindung mit einem Surface Pro-Gerät, auf dem Windows 8.1 ausgeführt wird, kann die Sitzung während der ersten Minute langsam sein, wenn "Sicherer Start" aktiviert ist. [#634382]
- Wenn Sie bei der Installation eines VDAs mit dem Produktinstallationsprogramm der grafischen Benutzeroberfläche Remote-PC-Zugriff aktivieren, werden zusätzliche Komponenten (Maschinenerstellungsdienste und Profilverwaltung) installiert. [#637741]. Verwenden Sie in diesem Release die Befehlszeile nur für Remote-PC-Zugriff-Bereitstellungen und ändern Sie nicht die Syntax für /components und /remotepc. Beispiel:

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE
"AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet
```

Wenn /remotepc vor /components steht, wird die Option /remotepc ignoriert. Weitere Informationen über Befehlszeilenoptionen finden Sie unter Installieren an der Befehlszeile.

### Windows Server 2016 Tech Preview

Eine Liste der Probleme bei Verwendung dieses Release von XenApp und XenDesktop unter Windows Server 2016 Tech Preview finden Sie im Windows Server 2016 Tech Preview-Forum (Anmeldung mit einem Citrix Konto erforderlich).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sonstige Komponenten

Bei separat auf den XenApp- und XenDesktop-Downloadseiten verfügbaren Komponenten sind folgende Probleme bekannt.

## Sitzungsaufzeichnung

- Die Installation der Sitzungsaufzeichnungsserverkomponenten schlägt mit den Fehlercodes 2503 und 2502 fehl. Lösung: Überprüfen Sie die Zugriffssteuerungsliste (ACL) im Ordner C:\windows\Temp, um sicherzustellen, dass für **Lokale Benutzer und Gruppen > Gruppen > Benutzer** Schreibberechtigung für diesen Ordner festgelegt ist. Falls nicht, fügen Sie die Schreibberechtigung manuell hinzu. [#611487]
- Da die Sitzungsaufzeichnung den Framehawk-Anzeigemodus nicht unterstützt, können Sitzungen in diesem Anzeigemodus nicht ordnungsgemäß aufgezeichnet und wiedergegeben werden. In diesem Modus aufgezeichnete Sitzungen enthalten ggf. keine Sitzungsaktivitäten. [#622085]
- Sie können Windows 7-Desktop-Sitzungen nicht ordnungsgemäß aufzeichnen, wenn über die XenDesktop-Siterichtlinie **Legacygrafikmodus** und über die Citrix Receiver für Windows-Richtlinie die datenträgerbasierte Zwischenspeicherung aktiviert sind. Die Aufzeichnungen erscheinen als schwarzer Bildschirm. Workaround: Deaktivieren Sie die datenträgerbasierte Zwischenspeicherung durch Bereitstellung mit einem Gruppenrichtlinienobjekt auf den Maschinen, auf denen Citrix Receiver für Windows installiert ist. Weitere Informationen zum Deaktivieren der datenträgerbasierten Zwischenspeicherung finden Sie unter http://support.citrix.com/article/CTX123169 und http://docs.citrix.com/en-us/receiver/windows/4-4/ica-overview-receiver-config/ica-import-icaclient-template-v2.html [#618237]
- Die Rollovereinstellung gilt nicht für VDI-Desktopsitzungen für XenDesktop 7.8 und 7.9 und den Sitzungsaufzeichnungsagent. Hier hat jede Aufzeichnungsdatei eine maximale Größe von 1 GB. Nach Erreichen dieses Limits werden Vorgänge nicht weiter aufgezeichnet. [#584890]
- Wenn von Maschinenerstellungsdienste (MCS) oder Provisioning Services mehrere VDAs mit einem konfigurierten Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt wird, erhalten die VDAs die gleiche QMID. Dies kann u. a. zu folgenden Problemen führen:
  - Sitzungen werden nicht aufgezeichnet, selbst wenn eine Aufzeichnungsvereinbarung akzeptiert wurde.
  - Das Sitzungsabmeldungssignal wird möglicherweise vom Sitzungsaufzeichnungsserver nicht empfangen, sodass die Sitzung permanent den Status "Live" hat. [#528678]

    Der Workaround zur Erstellung einer eindeutigen und persistenten QMID für jeden VDA hängt von der Bereitstellungsmethode ab.

    Keine zusätzliche Aktion ist erforderlich, wenn Desktopbetriebssystem-VDAs mit dem Sitzungsaufzeichnungsagent mit PVS 7.7 oder höher im statischen Desktopmodus erstellt wurden und festgelegt wurde, dass alle Änderungen mit einer separaten Personal vDisk oder einem lokalen Datenträger des VDAs persistent gemacht werden.

    Bei mit MCS oder PVS erstellten Serverbetriebssystem-VDAs oder bei mit MCS im statischen Desktopmodus erstellten dedizierten Desktopbetriebssystem-VDAs, für die festgelegt wurde, dass alle Änderungen mit einer separaten Personal vDisk oder einem lokalen Datenträger des VDAs persistent gemacht werden, verwenden Sie das Skript GenQMID.ps1 zum Ändern der QMID beim Systemstart.

    Bei Desktopbetriebssystem-VDAs, die mit MCS oder PVS erstellt und so konfiguriert wurden, dass alle Änderungen bei Abmeldung des Benutzers verworfen werden, verwenden Sie das Skript GenRandomQMID.ps1 zum Ändern der QMID beim Systemstart. Ändern Sie die Energieverwaltungsstrategie, um sicherzustellen, dass


© 1999-2017 Citrix Systems, Inc. All rights reserved.

vor Anmeldeversuchen der Benutzer genug VDAs ausgeführt werden.

Führen Sie zum Verwenden des Skripts folgende Schritte aus:

1. Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf "RemoteSigned" oder "Unrestricted" festgelegt ist.

   **Set-ExecutionPolicy RemoteSigned**

2. Erstellen Sie einen geplanten Task und legen Sie als Auslöser "Bei Systemstart" fest und für die Ausführung auf dem Computer mit dem Provisioning Services- oder MCS-Masterimage das Konto SYSTEM.

3. Fügen Sie den Befehl als Starttask hinzu.

   **powershell.exe -file C:\GenQMID.ps1**
   ODER
   **powershell .exe -file C:\GenRandomQMID.ps1**

**GenQMID.ps1 – Zusammenfassung**

1. Erstellen der QMID basierend auf dem Hashwert der Maschinen-UUID
2. Anhalten zugehöriger Dienste, einschließlich CitrixSmAudAgent und MSMQ
3. Starten der zuvor angehaltenen Dienste zum Anwenden der geänderten QMID

GENQMID.PS1-MUSTER: KOPIEREN

```
function ConvertHexStringToByte($theString)

{

    $bytes = New-Object Byte[] ($theString.Length / 2)

    for ($i = 0; $i -lt $theString.Length; $i += 2) {

        $bytes[$i / 2] = [System.Convert]::ToByte($theString.Substring($i, 2), 16)

    }

    return $bytes

}


Try {

    # Get UUID of machine
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    $strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Property UUID).UUID

    # Remove "-"
    $strUUID = $strUUID.ToString().Replace("-", "")

    # Convert string to bytes
    $UUID = ConvertHexStringToByte($strUUID)

    # Set UUID as QMId
    $new_QMID = $UUID
}
Catch {
    # IF exception occurred, just use MD5 digest of FQDN as QMID

    # Get FQDN
    $fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName

    # Calculate MD5 hash of FQDN
    $md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider

    # Set md5 digest as QMID
    $utf8 = new-object -TypeName System.Text.UTF8Encoding
    $new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Write new_QMID into registry

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name "QMId" -Value $new_QMID


# Restart MSMQ to adopt new QMId


# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

Restart-Service -force MSMQ


# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

    }

}
```

**GenRandomQMID.ps1 – Zusammenfassung**

1. Entfernen der aktuellen QMID aus der Registrierung
2. Hinzufügen von "SysPrep=1" zu HKLM\Software\Microsoft\MSMQ\Parameters
3. Anhalten zugehöriger Dienste, einschließlich CitrixSmAudAgent und MSMQ


© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Starten der zuvor angehaltenen Dienste zum Generieren einer zufälligen QMID

GENRANDOMQMID.PS1-MUSTER: KOPIEREN

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

}

}
```

- Beim Aufzeichnen einer Sitzung mit einer Auflösung über 4096 x 4096 ist die Aufzeichnungsanzeige u. U. fragmentiert. [#524973]
- Wenn Sie den Lizenztyp für XenApp oder XenDesktop ändern, wird die Änderung nicht sofort für die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sitzungsaufzeichnung wirksam. Workaround: Starten Sie den VDA-Computer neu. [#532393]

- Einschränkung für die Unterstützung vorab gestarteter Anwendungssitzungen durch die Sitzungsaufzeichnung [#561109]
  - Problem:
    - Wenn die aktive Richtlinie versucht, den Anwendungsnamen zuzuordnen, wird die in der vorab gestarteten Sitzung gestartete Anwendung nicht zugeordnet, sodass die Sitzung nicht aufgezeichnet wird.
    - Wenn die aktive Richtlinie jede Anwendung aufzeichnet und der Benutzer sich bei Windows Receiver anmeldet (zur gleichen Zeit, zu der die vorab gestartete Sitzung eingerichtet wird), erscheint eine Aufzeichnungsbenachrichtigung und die leere Sitzung sowie alle darin anschließend gestarteten Anwendungen werden aufgezeichnet.
  - Problemumgehung:
    - Veröffentlichen Sie die Anwendungen gemäß ihrer Aufzeichnungsrichtlinie in separaten Bereitstellungsgruppen. Verwenden Sie nicht den Anwendungsnamen als Aufzeichnungsbedingung. Damit wird sichergestellt, dass vorab gestartete Sitzungen aufgezeichnet werden. Benachrichtigungen werden jedoch weiterhin angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Nicht in diesem Release enthaltene Features

Jul 08, 2016

**Tipp:** Wenn die neueste Version, mit der Sie vertraut sind, XenApp 6.5 (oder eine Vorversion) ist, sollten Sie sich auch die hier beschriebenen Unterschiede bei Architektur, Terminologie und Elementen ansehen.

Die folgenden Features werden derzeit nicht bereitgestellt oder werden nicht mehr unterstützt.

- **Für Fingereingabe optimierten Desktop starten:** Diese Einstellung wurde für Windows 10-Maschinen deaktiviert. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Mobilerfahrung".
- **SecureICA-Verschlüsselung unter 128 Bit**: In Releases vor 7.x war eine Verschlüsselung von Clientverbindungen für Basic-, 40-Bit-, 56-Bit- und 128-Bit-Verschlüsselung durch SecureICA möglich. In Releases aber Version 7 steht die SecureICA-Verschlüsselung nur für die 128-Bit-Verschlüsselung zur Verfügung.
- **Legacydrucken**: Die folgenden Druckfunktionen werden für Releases 7.x nicht unterstützt:
  - Abwärtskompatibilität für DOS-Clients und 16-Bit-Drucker, einschließlich Legacy-Clientdruckernamen.
  - Unterstützung für mit Windows 95 und Windows NT verbundene Drucker, einschließlich verbesserter erweiterter Druckereigenschaften und Win32FavorRetainedSetting.
  - Möglichkeit zum Aktivieren oder Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker.
  - DefaultPrnFlag, eine Registrierungseinstellung für Server zum Aktivieren/Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker, die in Benutzerprofilen auf dem Server gespeichert werden.
- **Secure Gateway**: In Releases vor 7.x wurden mit Secure Gateway sichere Verbindungen zwischen dem Server und den Benutzergeräten hergestellt. Die Sicherung externer Verbindungen erfolgt nun mit NetScaler Gateway.
- **Spiegeln von Benutzern**: In Releases vor 7.x steuerten Administratoren die Benutzer-zu-Benutzer-Spiegelung mit Richtlinien. In 7.x-Releases ist das Spiegeln von Endbenutzern ein integriertes Feature in Director, wobei die Windows-Remoteunterstützung den Administratoren das Spiegeln und Beheben von Problemen auf nahtlos bereitgestellten Anwendungen und virtuellen Desktops gestattet.
- **Energie- und Kapazitätsverwaltung**: In Releases vor 7.x wurde mit der Energie- und Kapazitätsverwaltung der Stromverbrauch reduziert und die Serverkapazität verwaltet. Microsoft Configuration Manager ist das Ersatztool für diese Funktion.
- **Flash v1-Umleitung**: Bei Clients, die nicht die Flash-Umleitung der zweiten Generation unterstützen (einschließlich Citrix Receiver für Windows vor Version 3.0, Citrix Receiver für Linux 11.100 und Citrix Online-Plug-In 12.1) erfolgt ein Fallback auf serverseitige Wiedergabe für Legacyfeatures der Flash-Umleitung. VDAs in 7.x-Releases unterstützen die Flash-Umleitungsfeatures der zweiten Generation.
- **Lokales Textecho**: Dieses Feature wurde mit früheren Windows-Anwendungstechnologien zur Beschleunigung der Anzeige eingegebenen Texts auf Benutzergeräten bei Verbindungen mit hoher Latenz eingesetzt. Aufgrund von Verbesserungen am Grafiksubsystem und HDX SuperCodec ist dieses Feature in 7.x-Releases nicht enthalten.
- **SmartAuditor**: In Releases vor 7.x konnte mit SmartAuditor die Bildschirmaktivität einer Benutzersitzung aufgezeichnet werden. Ab Version 7.6 Feature Pack 1 wurde diese Funktion durch die Sitzungsaufzeichnung ersetzt.
- **Single Sign-On**: Dieses Feature zur Gewährleistung der Kennwortsicherheit wird für Windows 8- und Windows Server 2012-Umgebungen nicht unterstützt. Es wird noch für Windows 2008 R2- und Windows 7-Umgebungen unterstützt, ist aber nicht in 7.x-Releases enthalten. Es ist auf der Downloadwebsite von Citrix verfügbar: http://citrix.com/downloads.
- **Oracle-Datenbankunterstützung**: 7.x-Releases benötigen eine SQL Server-Datenbank.
- **Systemüberwachung und -wiederherstellung (HMR)**: In Releases vor 7.x konnten von HMR Tests auf den Servern einer Serverfarm durchgeführt werden, um deren Zustand zu überwachen und mögliche Integritätsrisiken zu ermitteln. In 7.x-Releases bietet Director eine zentrale Ansicht der Systemintegrität, da die Überwachungs- und Warnfunktionen für


© 1999-2017 Citrix Systems, Inc. All rights reserved.

die ganze Infrastruktur innerhalb der Director-Konsole dargestellt werden.

- **Benutzerdefinierte ICA-Dateien**: Benutzerdefinierte ICA-Dateien wurden verwendet, um direkte Verbindungen von Benutzergeräten (mit der ICA-Datei) zu einer bestimmten Maschine herzustellen. In 7.x-Releases ist dieses Feature standardmäßig deaktiviert, kann aber für die normale Verwendung mit einer lokalen Gruppe aktiviert werden, oder im Modus für hohe Verfügbarkeit verwendet werden, falls der Controller nicht mehr verfügbar ist.
- **Management Pack für System Center Operations Manager (SCOM) 2007**: Das Management Pack für die Überwachung der Aktivität der Farmen mit SCOM unterstützt 7.x-Releases nicht.
- **CNAME-Funktion**: Die CNAME-Funktion war in Versionen vor 7.x standardmäßig aktiviert. Bereitstellungen, die von CNAME-Einträgen für FQDN-Umleitung und von der Verwendung von NetBIOS-Namen abhängig sind schlagen möglicherweise fehl. In 7.x-Releases bietet stattdessen die automatische Aktualisierung von Delivery Controllern, durch die die Liste der Controller automatisch aktualisiert wird und VDAs automatisch benachrichtigt werden, wenn Controller der Site hinzugefügt und aus ihr entfernt werden. Das Feature für automatische Controller-Updates ist in den Citrix Richtlinien standardmäßig aktiviert, kann jedoch durch Erstellen einer Richtlinie deaktiviert werden. Alternativ können Sie die CNAME-Funktion in der Registrierung wieder aktivieren, um mit der vorhandenen Bereitstellung fortzufahren und FQDN-Umleitung und die Verwendung von NetBIOS-Namen zuzulassen. Weitere Informationen finden Sie unter CTX137960.
- **Assistent für schnelles Bereitstellen**: In Studio-Releases vor 7.x konnte mit dieser Option eine vollständig installierte XenDesktop-Bereitstellung schnell bereitgestellt werden. Durch den neuen vereinfachten Installations- und Konfigurationsworkflow in XenDesktop 7.x ist der Assistent für schnelles Bereitstellen nicht mehr nötig.
- **Konfigurationsdatei für Remote PC-Dienst und PowerShell-Skript für die automatische Verwaltung**: Remote PC ist jetzt in Studio und den Controller integriert.
- **Workflow Studio**: In Releases vor 7.x war Workflow Studio die grafische Oberfläche für den Aufbau von Workflows für XenDesktop. Das Feature wird in 7.x-Releases nicht unterstützt.
- **Farbtiefe**: In Studio-Releases vor 7.6 wurde die Farbtiefe in den Benutzereinstellungen einer Bereitstellungsgruppe angegeben. Ab Version 7.6 kann die Farbtiefe für Bereitstellungsgruppen über das PowerShell-Cmdlet "New-BrokerDesktopGroup" oder "Set-BrokerDesktopGroup" festgelegt werden.
- **Starten nicht-veröffentlichter Programme bei Clientverbindung**: In Releases vor 7.x wurde über diese Citrix Richtlinieneinstellung angegeben, ob Startanwendungen oder veröffentlichte Anwendungen über ICA oder RDP auf dem Server gestartet werden sollten. In 7.x-Releases wird mit dieser Einstellung nur festgelegt, ob Startanwendungen oder veröffentlichte Anwendungen über RDP auf dem Server gestartet werden.
- **Desktop starten**: In Releases vor 7.x wird mit dieser Citrix Richtlinieneinstellung angegeben, ob Benutzer, die keine Administratoren sind, eine Verbindung zu einer Desktopsitzung herstellen dürfen. In 7.x-Releases müssen Benutzer ohne Administratorrechte zur Gruppe der Benutzer mit direktem Zugriff für eine VDA-Maschine gehören, um Verbindungen zu Sitzungen auf diesem VDA herzustellen. Die Einstellung **Desktop starten** ermöglicht Benutzern ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zum VDA herzustellen. Die Einstellung **Desktop starten** hat keine Auswirkungen auf RDP-Verbindungen. Unabhängig von dieser Einstellung können Benutzer, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine RDP-Verbindung eine Verbindung zum VDA herstellen.

### Nicht in Citrix Receiver enthaltene Features oder Features mit anderen Standardwerten

- **COM-Portzuordnung**: Mit der COM-Portzuordnung wurde der Zugriff auf COM-Ports auf dem Benutzergerät erlaubt oder verhindert. Die COM-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Versionen von XenDesktop und XenApp ist die COM-Portzuordnung standardmäßig deaktiviert. Einzelheiten finden Sie unter Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung.
- **LPT-Portzuordnung**: Mit der LPT-Portzuordnung wird der Zugriff von Legacyanwendungen auf LPT-Ports gesteuert. Die LPT-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Releases ist die LPT-Portzuordnung standardmäßig


© 1999-2017 Citrix Systems, Inc. All rights reserved.

deaktiviert.

- **PCM-Audiocodec**: In 7.x-Releases wird der PCM-Audiocodec nur von HTML5-Clients unterstützt.
- **Unterstützung für Microsoft ActiveSync**
- **Proxyunterstützung für ältere Versionen**, dies umfasst:
  - Microsoft Internet Security und Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet-Proxyserver 4.0.14 (Windows Server 2003)
  - Squid-Proxyserver 3.1.14 (Ubuntu Linux Server 11.10)


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Hinweise zu Drittanbietern

Jul 08, 2016

Dieses Release von XenApp und XenDesktop enthält ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

- XenApp 7.9 und XenDesktop 7.9 Hinweise zu Drittanbietern
- FLEXnet Publisher Documentation Supplement: Third Party and Open Source Software used in FlexNet Publisher 11.13.1
- Linux Virtual Desktop Version 1.2 - Hinweise von Dritten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Systemanforderungen

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


- Delivery Controller
- Datenbanken
- Citrix Studio
- Citrix Director
- Virtual Delivery Agent (VDA) für Desktopbetriebssysteme
- Virtual Delivery Agent (VDA) für Serverbetriebssysteme
- Hosts/Virtualisierungsressourcen
- Funktionsebenen von Active Directory
- HDX
- Sitzungsaufzeichnung
- Universeller Druckserver
- Sonstiges


# Einführung

Die Systemanforderungen in diesem Dokument galten zum Zeitpunkt der Freigabe der Produktversion, Änderungen werden regelmäßig veröffentlicht. Nicht in diesem Dokument aufgeführte Systemanforderungen (z. B. StoreFront, Hostsysteme, Citrix Receiver und Plug-Ins oder Provisioning Services) werden in der jeweiligen Dokumentation behandelt.

**Wichtig:** Vor Beginn einer Installation lesen Sie Vorbereiten der Installation.

Sofern nicht anders angegeben, wird erforderliche Software (z. B. .NET und C++-Pakete) automatisch bereitgestellt, wenn die erforderlichen Versionen nicht auf der Maschine erkannt werden. Das Citrix Installationsmedium enthält außerdem einige erforderliche Softwarekomponenten.

Das Installationsmedium enthält mehrere Komponenten von Drittanbietern. Bevor Sie diese Citrix Software verwenden, überprüfen Sie, ob Sicherheitsupdates von Drittanbietern nötig sind und installieren Sie sie.

Die Speicherplatzangaben sind Schätzwerte und verstehen sich zuzüglich des für Produktimage, Betriebssystem und andere Software erforderlichen Speicherplatzes.

Wenn Sie die Kernkomponenten (Controller mit SQL Server Express, Studio, Director, StoreFront und Lizenzierung) auf einem Server installieren, benötigen Sie für die Evaluierung des Produkts mindestens 4 GB Arbeitsspeicher; mehr Speicher wird empfohlen, wenn Sie eine Umgebung für Benutzer ausführen. Die Leistung schwankt abhängig von der genauen Konfiguration, einschließlich der Anzahl der Benutzer, Anwendungen und Desktops sowie anderen Faktoren.

Informationen zur Globalisierung finden Sie unter CTX119253.

# Delivery Controller

Unterstützte Betriebssysteme:

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- Aktuelle Windows Server 2016 Technology Preview: Die Unterstützung für dieses Betriebssystem in diesem Release dient Evaluierungszwecken und ist nicht für Produktionsumgebungen vorgesehen.
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)
- Microsoft .NET Framework 4.5.2 (4.6 wird ebenfalls unterstützt)
- Windows PowerShell 2.0 (in Windows Server 2008 R2 enthalten) oder 3.0 (in Windows Server 2016 Technical Preview, Windows Server 2012 R2 und Windows Server 2012 enthalten)
- Visual C++ 2008 SP1 Redistributable Package
- Speicherplatz auf dem Datenträger: 100 MB

  Die Verwendung optionaler Features erhöht den Bedarf an Speicherplatz. Der erforderliche Speicherplatz für das standardmäßig aktivierte Verbindungsleasing hängt beispielsweise von der Anzahl Benutzer und Anwendungen und vom Modus ab: Bei 100.000 RDS-Benutzern mit 100 vor kurzem verwendeten Anwendungen werden ca. 3 GB für das Verbindungsleasing benötigt, bei Bereitstellungen mit mehr Anwendungen ist ggf. mehr Speicherplatz erforderlich. Bei dedizierten VDI-Desktops benötigen 40.000 Desktops mindestens 400-500 MB. Auf jeden Fall empfiehlt es sich, mehrere GB an zusätzlichem Speicherplatz bereitzustellen.

# Datenbanken

Unterstützte Versionen von Microsoft SQL Server für die Datenbanken für Sitekonfiguration, Konfigurationsprotokollierung und Überwachung:

- SQL Server 2016, Express, Standard und Enterprise Edition.
- SQL Server 2014 bis SP2, Express, Standard und Enterprise Edition.
- SQL Server 2012 bis SP3, Express, Standard und Enterprise Edition. Standardmäßig wird SQL Server 2012 SP2 Express zusammen mit dem Controller installiert, wenn keine unterstützte SQL Server-Installation erkannt wird.
- SQL Server 2008 R2 SP2 und SP3, Express, Standard, Enterprise und Datacenter Edition.

Die folgenden Datenbankfeatures werden unterstützt (außer bei SQL Server Express, das nur den eigenständigen Modus unterstützt):

- SQL Server-Cluster-Instanzen
- SQL Server-Spiegelung
- SQL Server 2012-AlwaysOn-Verfügbarkeitsgruppen

Die Windows-Authentifizierung ist für Verbindungen zwischen dem Controller und der SQL Server-Datenbank erforderlich.

Weitere Informationen finden Sie in den Artikeln Datenbanken und CTX114501.

# Citrix Studio

Unterstützte Betriebssysteme:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Windows 10, Professional, Enterprise und Education Edition
- Windows 8.1, Professional und Enterprise Edition
- Windows 8, Professional und Enterprise Edition
- Windows 7, Professional, Enterprise und Ultimate Edition
- Aktuelle Windows Server 2016 Technology Preview: Die Unterstützung für dieses Betriebssystem in diesem Release dient Evaluierungszwecken und ist nicht für Produktionsumgebungen vorgesehen.
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Speicherplatz auf der Datenträger: 75 MB
- Microsoft .NET Framework 4.5.2 (4.6 wird ebenfalls unterstützt)
- Microsoft .NET Framework 3.5 SP1 (nur Windows Server 2008 R2 und Windows 7)
- Microsoft Management Console 3.0 (in allen unterstützten Betriebssystemen enthalten)
- Windows PowerShell 2.0 (in Windows 7 und Windows Server 2008 R2 enthalten) oder 3.0 (in Windows 10, Windows 8.1, Windows 8, Windows Server 2016 Technology Preview, Windows Server 2012 R2 und Windows Server 2012 enthalten)

# Citrix Director

Unterstützte Betriebssysteme:

- Aktuelle Windows Server 2016 Technology Preview: Die Unterstützung für dieses Betriebssystem in diesem Release dient Evaluierungszwecken und ist nicht für Produktionsumgebungen vorgesehen.
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Speicherplatz auf dem Datenträger: 140 MB
- Microsoft .NET Framework 4.5.2 (4.6 wird ebenfalls unterstützt)
- Microsoft .NET Framework 3.5 SP1 (nur Windows Server 2008 R2)
- Microsoft Internetinformationsdienste (IIS) 7.0 und ASP.NET 2.0. Stellen Sie sicher, dass der Static Content-Rollendienst für die IIS-Serverrolle installiert ist. Wenn diese Komponenten nicht auf Ihrem Server installiert sind, werden Sie möglicherweise aufgefordert, das Windows Server-Installationsmedium einzulegen. Sie werden dann installiert.

Anforderungen für eine System Center Operations Manager-Integration:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Unterstützte Browser zum Anzeigen von Director:

- Internet Explorer 11. Sie können Internet Explorer 10 verwenden, doch die von Microsoft unterstützte und von Citrix empfohlene Version ist Version 11. Der Kompatibilitätsmodus wird für Internet Explorer nicht unterstützt. Für den Zugriff auf Director müssen Sie die empfohlenen Webbrowsereinstellungen verwenden. Akzeptieren Sie bei der Installation von Internet Explorer die Standardeinstellung zur Verwendung der empfohlenen Sicherheits- und

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Kompatibilitätseinstellungen. Wenn der Browser bereits ohne die empfohlenen Einstellungen installiert ist, navigieren Sie auf "Extras > Internetoptionen > Erweitert" > Zurücksetzen" und folgen Sie den Anweisungen.
- Microsoft Edge
- Firefox ESR (Extended Support Release)
- Chrome

Die empfohlene Bildschirmauflösung für die Anzeige von Director ist 1366 x 1024.

# Virtual Delivery Agent (VDA) für Desktopbetriebssysteme

Unterstützte Betriebssysteme:

- Windows 10, Professional, Enterprise und Education Edition Folgende Features werden unter Windows 10 nicht unterstützt: GPU-Beschleunigung für ein VDA im Standardmodus, Desktopgestaltungsumleitung, Legacygrafikmodus, sicherer Start (wird nur für Remote-PC-Zugriff unterstützt) und die Veröffentlichung universeller Windows-Anwendungen mit VM-gehosteten Anwendungen.
- Windows 8.1, Professional und Enterprise Edition
- Windows 8, Professional und Enterprise Edition
- Windows 7 SP1, Professional, Enterprise und Ultimate Edition

Zur Verwendung des Server-VDI-Features können Sie über die Befehlszeilenschnittstelle einen VDA für Windows-Desktopbetriebssysteme auf einem unterstützten Serverbetriebssystem installieren. Weitere Informationen finden Sie im Artikel Server-VDI.

- Aktuelle Windows Server 2016 Technology Preview: Die Unterstützung für dieses Betriebssystem in diesem Release dient Evaluierungszwecken und ist nicht für Produktionsumgebungen vorgesehen.
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Microsoft .NET Framework 4.5.2 (4.6 wird ebenfalls unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows 7)
- Microsoft Visual C++ 2008 SP1, 2010 SP1 und 2013 Runtimes (32-Bit und 64-Bit)

Remote-PC-Zugriff verwendet diesen VDA, den Sie auf physischen Büro-PCs installieren.

Dieser Virtual Delivery Agent (VDA) unterstützt den sicheren Start für XenDesktop-Remote-PC-Zugriff unter Windows 10 und 8.1.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfeatures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows-Desktopbetriebssystemen ist Media Foundation bereits


© 1999-2017 Citrix Systems, Inc. All rights reserved.

installiert und kann nicht entfernt werden. Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen.

Bei der VDA-Installation können Sie entscheiden, ob Sie die HDX 3D Pro-Version des VDAs für Windows-Desktopbetriebssysteme installieren möchten. Diese Version eignet sich besonders für die Verwendung mit DirectX- und OpenGL-gesteuerten Anwendungen sowie mit Rich Media-Inhalten wie Video. Weitere Informationen zur Unterstützung finden Sie im Abschnitt HDX 3D Pro.

Sie können einen VDA der aktuellen Version nicht auf einer Maschine unter Windows XP oder Windows Vista installieren. Sie können bei diesen Betriebssystemen jedoch bei Bedarf eine Vorversion von Virtual Desktop Agent installieren. Einzelheiten hierzu finden Sie unter CTX140941. Die Version von Remote-PC-Zugriff in diesem Release wird nicht auf Windows Vista-Betriebssystemen unterstützt.

# Virtual Delivery Agent (VDA) für Serverbetriebssysteme

Unterstützte Betriebssysteme:

- Aktuelle Windows Server 2016 Technology Preview: Die Unterstützung für dieses Betriebssystem in diesem Release dient Evaluierungszwecken und ist nicht für Produktionsumgebungen vorgesehen.
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Das Installationsprogramm stellt die folgenden Anforderungen automatisch bereit, die auch auf den Citrix Installationsmedien in den Ordnern \Support zur Verfügung stehen:

- Microsoft .NET Framework 4.5.2 (4.6 wird ebenfalls unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)
- Microsoft Visual C++ 2008 SP1, 2010 SP1 und 2013 Runtimes (32-Bit und 64-Bit)

Das Installationsprogramm installiert und aktiviert automatisch die Rollendienste für Remotedesktopdienste, wenn sie nicht bereits installiert und aktiviert sind.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfeatures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2 wird Media Foundation über den Server-Manager installiert (bei Windows Server 2012 R2 und Windows Server 2012: ServerMediaFoundation, bei Windows Server 2008 R2: DesktopExperience). Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen.

# Hosts/Virtualisierungsressourcen

Einige XenApp- und XenDesktop-Features werden möglicherweise nicht auf allen Hostplattformen bzw. allen Plattformversionen unterstützt. AppDisks werden beispielsweise auf XenServer- und VMware-Hosts unterstützt. Weitere Informationen finden Sie in der Dokumentation zu dem jeweiligen Feature.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

CTX131239 enthält zusätzliche Supportinformationen zur Hypervisorversion.

Unterstützte Hostplattformen:

XenServer

- XenServer 6.5 und SP1
- XenServer 6.2 SP1 und Hotfixes (Sie müssen SP1 anwenden, damit die Anwendung zukünftiger Hotfixes möglich ist)
- XenServer 6.1

VMware vSphere: Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.

- VMware vSphere 6.0 und Updates 1 und 2
- VMware vSphere 5.5 und Update 1 bis 3
- VMware vSphere 5.1 Updates 2 und 3
- VMware vSphere 5.0 Updates 2 und 3
- VMware vCenter 5.5-/6-Gerät

System Center Virtual Machine Manager: enthält alle Versionen von Hyper-V, die mit den unterstützten Versionen von System Center Virtual Machine Manager registriert werden können.

- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5: Wenn Sie diese Plattform verwenden, stehen verschiedene XenApp- und XenDesktop-Features nicht zur Verfügung; weitere Informationen finden Sie unter CTX202032. Weitere Informationen zur Verwendung des Produkts mit Acropolis finden Sie unter https://portal.nutanix.com/#/page/docs.

Unterstützte Cloudumgebungen:

Amazon Web Services (AWS)

- Sie können Anwendungen und Desktops auf unterstützten Windows Server-Betriebssystemen bereitstellen.
- SQL Server 2012 Enterprise ist für AWS nicht verfügbar.
- AWS bietet keine Desktopbetriebssysteminstanzen.
- Amazon Relational Database Service (RDS) wird nicht unterstützt.
- Weitere Informationen finden Sie unter Citrix XenDesktop auf AWS.

Citrix CloudPlatform

- Die unterstützte Mindestversion ist 4.2.1 mit Hotfixes 4.2.1-4.
- Bereitstellungen wurden mit XenServer 6.2 (mit Service Pack 1 und Hotfix XS62ESP1003) und vSphere 5.1-Hypervisors getestet.
- CloudPlatform unterstützt keine Hyper-V-Hypervisors.
- CloudPlatform 4.3.0.1 unterstützt VMware vSphere 5.5.
- Weitere Informationen finden Sie in der CloudPlatform-Dokumentation (einschließlich den Versionshinweisen zu Ihrer CloudPlatform-Version).

Microsoft Azure

Das Wake-On-LAN-Feature von Remote-PC-Zugriff erfordert Microsoft System Center Configuration Manager 2012.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# Funktionsebenen von Active Directory

Die folgenden Funktionsebenen werden für Active Directory-Gesamtstrukturen und -Domänen unterstützt:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Natives Windows 2000 (auf Domänencontrollern nicht unterstützt)

# HDX

UDP-Audio für Multistream-ICA wird unter Citrix Receiver für Windows und Citrix Receiver für Linux 13 unterstützt.

Die Echounterdrückung wird unter Receiver für Windows unterstützt.

Siehe Informationen zu Unterstützung und Anforderungen für HDX unten.

## HDX-Desktopgestaltungsumleitung

Das Windows-Benutzergerät bzw. der Thin Client muss Folgendes unterstützen oder enthalten:

- DirectX 9
- Pixel Shader 2.0 (in Hardware unterstützt)
- 32 Bit pro Pixel
- 1,5 GHz Prozessor (32-Bit oder 64-Bit)
- 1 GB RAM
- 128 MB Videospeicher auf der Grafikkarte oder einem integrierten Grafikprozessor

HDX überprüft das Windows-Gerät auf die erforderlichen GPU-Anforderungen und schaltet dann ggf. automatisch auf serverseitige Desktopgestaltung um. Geräte, die die erforderlichen GPU-Anforderungen erfüllen aber nicht die benötigte Prozessorgeschwindigkeit oder RAM-Spezifikationen haben, müssen in der GPO-Gruppe der Geräte erfasst werden, die von der Desktopgestaltungsumleitung ausgeschlossen sind.

Als Mindestausstattung ist eine verfügbare Bandbreite von 1,5 MBit/s erforderlich, empfohlen werden 5 MBit/s. Die Werte schließen End-to-End-Latenz ein.

## HDX und Windows Media-Bereitstellung

Für den clientseitigen Abruf von Windows Media-Inhalten, die Windows Media-Umleitung und die Windows Media-Multimediatranscodierung in Echtzeit werden folgende Clients unterstützt: Citrix Receiver für Windows, Citrix Receiver für iOS und Citrix Receiver für Linux.

Zur Verwendung des clientseitigen Inhaltsabrufs von Windows Media auf Windows 8-Geräten legen Sie Citrix Multimedia Redirector als Standardprogramm fest: Navigieren Sie zu **Systemsteuerung > Programme > Standardprogramme > Standardprogramme festlegen**, wählen Sie **Citrix Multimedia Redirector** und klicken Sie auf **Dieses Programm als Standard festlegen** oder auf **Standards für dieses Programm auswählen**. Für die GPU-Transcodierung ist ein NVIDIA

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

CUDA-fähiger GPU mit Compute Capability 1.1 oder höher erforderlich. Siehe http://developer.nvidia.com/cuda/cuda-gpus.

### HDX-Flash-Umleitung

Die folgenden Clients und Adobe Flash Player-Versionen werden unterstützt:

- Citrix Receiver für Windows: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for Other Browsers, diese Version wird auch als NPAPI (Netscape Plugin Application Programming Interface) Flash Player bezeichnet.
- Citrix Receiver für Linux: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for other Linux oder Adobe Flash Player for Ubuntu.
- Citrix Online Plug-In 12.1: Für Legacyfeatures der Flash-Umleitung wird Adobe Flash Player für Windows Internet Explorer benötigt (auch ActiveX Player genannt).

Die Hauptversionsnummer von Flash Player auf dem Benutzergerät muss größer oder gleich der Hauptversionsnummer von Flash Player auf dem Server sein. Wenn eine ältere Version oder gar keine Version von Flash Player auf dem Benutzergerät installiert ist, werden Flash-Inhalte auf dem Server wiedergegeben.

Die Maschinen, auf denen VDAs ausgeführt werden, erfordern Folgendes:

- Adobe Flash Player für Windows Internet Explorer (ActiveX Player)
- Internet Explorer 11 (im Modus "Nicht-moderne-Oberfläche"). Sie können Internet Explorer 7-10 verwenden, doch die von Microsoft unterstützte und von Citrix empfohlene Version ist Version 11. Flash-Umleitung erfordert Internet Explorer auf dem Server; mit anderen Browsern werden Flash-Inhalte auf dem Server wiedergegeben.
- Der geschützte Modus muss in Internet Explorer deaktiviert sein (Extras > Internetoptionen > Registerkarte "Sicherheit" > Kontrollkästchen "Geschützten Modus aktivieren" deaktiviert). Starten Sie Internet Explorer neu, damit die Änderung wirksam wird.

### HDX 3D Pro

Wenn Sie einen VDA für Windows-Desktopbetriebssysteme installieren, können Sie die Version HDX 3D Pro installieren.

Auf der physischen bzw. virtuellen Maschine, auf der die Anwendung gehostet wird, kann GPU-Passthrough oder Virtual GPU (vGPU) verwendet werden:

- GPU-Passthrough steht mit Citrix XenServer zur Verfügung. GPU-Passthrough ist auch mit VMware vSphere und VMware ESX verfügbar und wird in diesem Zusammenhang als vDGA (virtual Direct Graphics Acceleration) bezeichnet.
- vGPU ist mit Citrix XenServer und VMware vSphere verfügbar. Weitere Informationen finden Sie unter www.citrix.com/go/vGPU (Anmeldeinformationen für Citrix My Account erforderlich).

Als Minimalausstattung für den Hostcomputer empfiehlt Citrix 4 GB RAM und vier virtuelle CPUs mit einer Taktfrequenz von 2,3 GHz.

Grafikprozessor (GPU):

- Im Hinblick auf CPU-basierte Komprimierung, einschließlich verlustfreier Komprimierung, unterstützt HDX 3D Pro alle Grafikkarten auf dem Hostcomputer, die mit der bereitgestellten Anwendung kompatibel sind.
- Zur Optimierung des GPU-Framepufferzugriffs mit der NVIDIA GRID-API kann HDX 3D Pro mit unterstützten NVIDIA GRID-Karten verwendet werden (siehe NVIDIA GRID). NVIDIA GRID liefert eine hohe Framerate und dadurch eine sehr interaktive Benutzererfahrung.
- Zur Optimierung des GPU-Framepufferzugriffs mit dem Intel Media-SDK, kann HDX 3D Pro mit unterstützten Intel-

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Hardwareplattformen und Intel Iris Pro Graphics verwendet werden. Zu den unterstützten Intel-Prozessoren gehören Intel Core-Prozessoren der fünften Generation und Intel Core i5-Prozessoren der sechsten Generation.
- Zu den Anforderungen für HDX 3D Pro zur Verwendung von vGPU mit XenServer gehören die Grafikkarten NVIDIA GRID K1 und K2 (siehe NVIDIA GRID).

Benutzergerät:

- HDX 3D Pro unterstützt alle Monitorauflösungen, die von dem GPU auf dem Hostcomputer unterstützt werden. Um mit den empfohlenen Minimalspezifikationen für Benutzergeräte und GPUs eine optimale Leistung zu erzielen, empfiehlt Citrix jedoch eine maximale Monitorauflösung für Benutzergeräte von 1920 x 1200 Pixeln für LAN-Verbindungen sowie von 1280 x 1024 Pixeln für WAN-Verbindungen.
- Als Mindestausstattung für Benutzergeräte empfiehlt Citrix mindestens 1 GB RAM und eine CPU mit einer Taktfrequenz von 1,6 GHz. Zur Verwendung des standardmäßigen Tiefenkomprimierungscodecs, der bei Verbindungen mit geringer Bandbreite erforderlich ist, ist eine leistungsfähigere CPU erforderlich, es sei denn, die Decodierung erfolgt in der Hardware. Zur Erzielung der optimalen Leistung empfiehlt Citrix die Ausstattung von Benutzergeräten mit mindestens 2 GB RAM und einer Dual-Core-CPU mit einer Taktfrequenz von mindestens 3 GHz.
- Bei Multimonitorzugriff empfiehlt Citrix Benutzergeräte mit Vierkern-CPUs.
- Benutzergeräte benötigen keinen GPU für den Zugriff auf Desktops oder Anwendungen, die mit HDX 3D Pro bereitgestellt werden.
- Citrix Receiver muss installiert sein.

Weitere Informationen finden Sie unter HDX 3D Pro und www.citrix.com/xenapp/3d.

### HDX-Videokonferenzen – Anforderungen für Webcam-Videokomprimierung

Unterstützte Clients: Citrix Receiver für Windows, Citrix Receiver für Mac und Citrix Receiver für Linux

Unterstützte Videokonferenzanwendungen:

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google + Hangouts
- IBM Sametime
- Media Foundation-basierte Videoanwendungen auf Windows 8.x, Windows Server 2012 und Windows Server 2012 R2
- Microsoft Lync 2010 und 2013
- Für Microsoft Office Communicator:
- Microsoft Skype 6.7

Zum Verwenden von Skype auf einem Windows-Client bearbeiten Sie die Registrierung auf Client und Server folgendermaßen:

Clientregistrierungsschlüssel HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

Name: DefaultHeight, Typ: REG_DWORD, Wert: 240

Name: DefaultWidth, Typ: REG_DWORD, Wert: 320

Serverregistrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Kompatibilität

Name: skype.exe, Typ: REG_DWORD, Wert: 0

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-verschlüsselungsfähige Webcams senken die clientseitige CPU-Nutzung.
- Webcam-Treiber (möglichst vom Kamerahersteller)

# Sitzungsaufzeichnung

In diesem Abschnitt werden die Systemanforderungen für folgende Komponenten aufgelistet:

Verwaltungskomponenten der Sitzungsaufzeichnung

Sitzungsaufzeichnungsagent

Sitzungsaufzeichnungsplayer

### Verwaltungskomponenten der Sitzungsaufzeichnung

Die Verwaltungskomponenten der Sitzungsaufzeichnung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole) können auf demselben oder mehreren Servern installiert werden.

## Datenbank für die Sitzungsaufzeichnung

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Unterstützte Microsoft SQL Server-Versionen:

- Microsoft SQL Server 2014 Enterprise, Express und Standard
- Microsoft SQL Server 2012 SP2 Enterprise und Express Edition
- Microsoft SQL Server 2008 R2 SP3 Enterprise und Express Edition

Voraussetzung: .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.2 oder 4.6.

## Sitzungsaufzeichnungsserver

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Sie müssen die Voraussetzungen vor dem Sitzungsaufzeichnungsserver installieren. Fügen Sie im Server-Manager die IIS-Rolle hinzu und wählen Sie folgende Optionen:

- Anwendungsentwicklung > ASP.NET 4.5 (Server 2012 und Server 2012 R2), ASP.NET (Server 2008 R2). Andere Komponenten werden automatisch ausgewählt; klicken Sie auf **Hinzufügen**, um die erforderlichen Rollen zu

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

übernehmen.
- Sicherheit > Windows-Authentifizierung
- Verwaltungsprogramme > IIS 6-Verwaltungskompatibilität: IIS 6-Metabasiskompatibilität, IIS 6-WMI-Kompatibilität, IIS 6-Skriptingtools, IIS 6-Verwaltungskonsole

Weitere Anforderungen:

- .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.2 oder 4.6.
- Wenn der Sitzungsaufzeichnungsserver HTTPS als Kommunikationsprotokoll verwendet, fügen Sie ein gültiges Zertifikat hinzu. Die Sitzungsaufzeichnung verwendet in der Standardeinstellung HTTPS; dies wird von Citrix empfohlen.
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung.

## Richtlinienkonsole für die Sitzungsaufzeichnung

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Voraussetzung: .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.2 oder 4.6.

### Sitzungsaufzeichnungsagent

Installieren Sie den Sitzungsaufzeichnungsagent auf jedem XenApp-Server, auf dem Sie Sitzungen aufzeichnen möchten.

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8,1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Anforderungen:

- XenApp 7.8 oder XenDesktop 7.8 mit Platinum-Lizenz
- .NET Framework Version 4.5.2 oder 4.6
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung

### Sitzungsaufzeichnungsplayer

Unterstützte Betriebssysteme:

- Microsoft Windows 10
- Microsoft Windows 8,1
- Microsoft Windows 8


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft Windows 7 SP1

Voraussetzung: .NET Framework Version 3.5 SP1 (nur Windows 7), 4.5.2 oder 4.6

Für optimale Ergebnisse sollten Sie den Sitzungsaufzeichnungsplayer auf einer Arbeitsstation installieren, die folgende Anforderungen erfüllt:

- Eine Bildschirmauflösung von 1024 x 768
- Eine Farbtiefe von mindestens 32 Bit
- Mindestens 1GB RAM, größere RAM- und CPU-/GPU-Ressourcen können die Leistung bei der Wiedergabe grafikintensiver Aufzeichnungen verbessern, insbesondere, wenn die Aufzeichnungen viele Animationen enthalten.

Die Reaktionszeit bei der Suche hängt von der Größe der Aufzeichnung und der Computerhardware ab.

# Universeller Druckserver

Der universelle Druckserver umfasst Client- und Serverkomponenten. Die UPsClient-Komponente ist in der VDA-Installation enthalten. Die UPsServer-Komponente wird auf jedem Druckserver installiert, auf dem die freigegebenen Drucker gespeichert sind, die Sie mit dem universellen Druckertreiber von Citrix in Benutzersitzungen bereitstellen möchten.

Die UpsServer-Komponente wird unter folgenden Betriebssystemen unterstützt:

- Windows Server 2012 R2 und 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 (32 Bit)

Voraussetzung: Microsoft Visual C++ 2013 Runtime

Für VDAs für Windows-Serverbetriebssysteme erfordert die Benutzerauthentifizierung bei Druckvorgängen, dass der universelle Druckserver in der gleichen Domäne ist wie der VDA.

Auch eigenständige Client- und Server-Komponentenpakete stehen zum Download zur Verfügung.

Weitere Informationen finden Sie im Artikel Bereitstellen von Druckern.

# Sonstiges

Gemischte DPI-Werte bei mehreren Monitoren: Die Verwendung verschiedener DPI-Werte bei mehreren Monitoren wird in Citrix XenDesktop- und XenApp-Umgebungen nicht unterstützt. Sie können den DPI-Wert (Skalierung in %) unter "Windows-Systemsteuerung" > "Anzeige" überprüfen. Wenn Sie ein Windows 8.1- oder Windows 10-Clientgerät verwenden, können Sie unter "Windows-Systemsteuerung > Anzeige" mit der Option "Manuell eine Skalierungsstufe für alle Anzeigegeräte auswählen" die Monitore entsprechend konfigurieren. Weitere Informationen finden Sie unter CTX201696. Citrix empfiehlt die Installation der Komponentensoftwareversionen auf dem Installationsmedium für dieses Release (bzw. ein Upgrade auf diese Versionen).

- StoreFront erfordert 2 GB Arbeitsspeicher. Informationen zu Systemanforderungen finden Sie in der Dokumentation von StoreFront. StoreFront 2.6 ist die in diesem Release unterstützte Mindestversion.
- Wenn Sie Provisioning Services mit diesem Release verwenden, wird als Mindestversion Provisioning Services 7.0


© 1999-2017 Citrix Systems, Inc. All rights reserved.

unterstützt.

- Citrix Lizenzserver erfordert 40 MB Speicherplatz auf dem Datenträger. Informationen zu den Systemanforderungen finden Sie in der Dokumentation der Lizenzierung. Es wird nur Citrix Lizenzserver für Windows unterstützt. Die unterstützte Mindestversion ist 11.13.1.

Die Microsoft-Gruppenrichtlinien-Verwaltungskonsole ist erforderlich, wenn Sie Citrix Richtlinieninformationen in Active Directory und nicht in der Sitekonfigurationsdatenbank speichern. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Die Verwendung mehrerer Netzwerkkarten wird nicht unterstützt.

Standardmäßig wird zusammen mit einem VDA Citrix Receiver für Windows installiert. Weitere Informationen finden Sie in der Dokumentation von Citrix Receiver für Windows.

Informationen zu unterstützten Versionen von Microsoft App-V finden Sie im Artikel App-V.

Informationen zu unterstützten Browsern für den lokalen App-Zugriff finden Sie im Artikel Lokaler App-Zugriff.

Clientordnerumleitung – unterstützte Betriebssysteme:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012 und Windows Server 2012 R2
- Client (mit der aktuellen Version von Citrix Receiver für Windows): Windows 7, Windows 8, und Windows 8.1

Gemischte DPI-Werte bei mehreren Monitoren: Die Verwendung verschiedener DPI-Werte bei mehreren Monitoren wird in Citrix XenDesktop- und XenApp-Umgebungen nicht unterstützt. Sie können den DPI-Wert (Skalierung in %) unter "Windows-Systemsteuerung" > "Anzeige" überprüfen. Wenn Sie ein Windows 8.1- oder Windows 10-Clientgerät verwenden, können Sie unter "Windows-Systemsteuerung > Anzeige" mit der Option **Manuell eine Skalierungsstufe für alle Anzeigegeräte auswählen** die Monitore entsprechend konfigurieren. Weitere Informationen finden Sie unter CTX201696.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Technische Übersicht

Aug 17, 2016

XenApp und XenDesktop sind Virtualisierungslösungen, die IT die Steuerung von virtuellen Maschinen, Anwendungen sowie von der Lizenzierung und Sicherheit ermöglichen und gleichzeitig Benutzern von überall Zugriff mit jedem Gerät bieten.

XenApp und XenDesktop ermöglichen Folgendes:

- Endbenutzer können Anwendungen und Desktops unabhängig vom Betriebssystem und von der Benutzeroberfläche eines Geräts ausführen.
- Administratoren können Netzwerke verwalten und Zugriff von ausgewählten Geräten oder allen Geräten gewähren oder einschränken.
- Administratoren können ein ganzes Netzwerk von einem Datencenter aus verwalten.

XenApp und XenDesktop haben eine einheitliche Architektur, die FlexCast Management Architecture (FMA) genannt wird. Die Hauptfunktion von FMA umfasst die Ausführung mehrerer Versionen von XenApp oder XenDesktop auf einer einzigen Site und die Bereitstellung von integriertem Provisioning.

# Hauptkomponenten von FMA

Eine typische XenApp- oder XenDesktop-Umgebung besteht aus einigen technischen Hauptkomponenten, die interagieren, wenn Benutzer Verbindungen zu Anwendungen und Desktops herstellen, und Daten über die Siteaktivität erfassen.

**Citrix Receiver:** Softwareclient, der auf dem Benutzergerät installiert ist. Er stellt die Verbindung zur virtuellen Maschine über TCP-Port 80 oder 443 her und kommuniziert mit StoreFront über die StoreFront-Dienst-API.

**Citrix StoreFront:** Benutzeroberfläche, mit der Benutzer authentifiziert werden. Sie dient zur Verwaltung von Anwendungen und Desktops und zum Hosten des Anwendungsstores. StoreFront kommuniziert mit dem Delivery Controller mit XML.

**Delivery Controller:** zentrale Verwaltungskomponente einer XenApp- oder XenDesktop-Site. Sie besteht aus Diensten, die Ressourcen, Anwendungen und Desktops verwalten und die Last der Benutzerverbindungen optimieren und ausgleichen.

**Virtual Delivery Agent (VDA):** Agent, der auf Maschinen installiert ist, auf denen Windows Server- oder Windows-Desktopbetriebssysteme ausgeführt werden. Er gewährleistet, dass diese Maschinen und die von ihnen gehosteten Ressourcen Benutzern zur Verfügung gestellt werden können. Auf Windows-Serverbetriebssystemmaschinen ermöglichen VDAs das Hosten mehrerer Verbindungen für mehrere Benutzer und sind mit den Benutzern über einen der folgenden Ports verbunden:

- TCP-Port 80 oder Port 443, wenn TLS aktiviert ist
- TCP-Port 2598, wenn Citrix Gateway Protocol (CGP) aktiviert ist (für Sitzungszuverlässigkeit)
- TCP-Port 1494, wenn CGP deaktiviert ist oder wenn der Benutzer eine Verbindung über einen Legacyclient herstellt

**Brokerdienst:** Delivery Controller-Dienst, der protokolliert, welche Benutzer wo angemeldet sind, welche Sitzungsressourcen die Benutzer nutzen und ob Benutzer sich erneut mit vorhandenen Anwendungen verbinden müssen. Der Brokerdienst führt PowerShell aus und kommuniziert mit dem Broker Agent über TCP-Port 80. Er kann TCP-Port 443 nicht verwenden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Broker-Agent:** Agent, der mehrere Plug-Ins hostet und Echtzeitdaten sammelt. Der Broker Agent ist auf dem VDA und mit dem Controller über TCP-Port 80 verbunden. Er kann TCP-Port 443 nicht verwenden.

**Überwachungsdienst:** Komponente des Delivery Controllers, die historische Daten sammelt und diese standardmäßig in der Sitedatenbank speichert. Der Monitor Service kommuniziert über TCP-Port 80 oder 443.

**ICA-Datei/Stack:** gebündelte Benutzerinformationen, die für die Verbindung mit dem VDA erforderlich sind.

**Sitedatenbank:** Microsoft SQL-Datenbank, in der Daten für den Delivery Controller (Siterichtlinien, Maschinenkataloge, Bereitstellungsgruppen etc.) gespeichert werden.

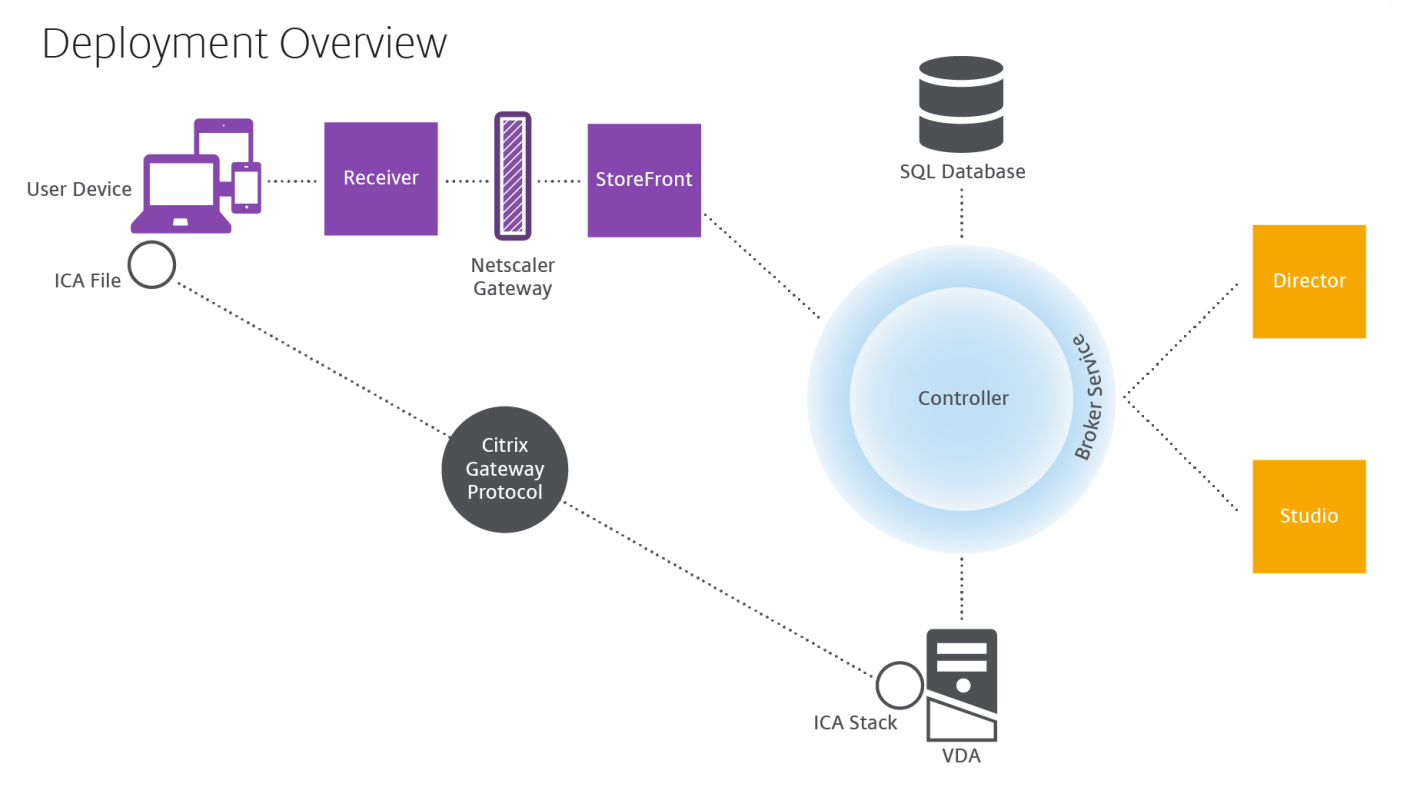
**NetScaler Gateway:** Datenzugriffslösung, die sicheren Zugriff von innerhalb oder außerhalb der LAN-Firewall durch zusätzliche Anmeldeinformationen gewährleistet.

**Citrix Director:** webbasiertes Tool, das Administratoren und Helpdeskpersonal den Zugriff auf Echtzeitdaten vom Broker-Agent, historische Daten von der Sitedatenbank und HDX-Daten von NetScaler für die Problembehandlung und den Support bietet. Director kommuniziert mit dem Controller über TCP-Port 80 oder 443.

**Citrix Studio:** Verwaltungskonsole, mit der Administratoren Sites konfigurieren und verwalten und die den Zugriff auf Echtzeitdaten vom Broker-Agent ermöglicht. Studio kommuniziert mit dem Controller über TCP-Port 80.

## Funktionsweise typischer Bereitstellungen

XenApp- und XenDesktop-Sites bestehen aus Maschinen mit dedizierten Rollen, die Skalierbarkeit, hohe Verfügbarkeit und Failover gewährleisten und auf diese Weise eine inhärent sichere Lösung bieten. Eine XenApp- oder XenDesktop-Site besteht aus Server- und Desktopmaschinen mit installierten VDAs und dem Delivery Controller, der den Zugriff verwaltet.




Durch den VDA können Benutzer Verbindungen mit Desktops und Anwendungen herstellen. Er ist auf Server- oder Desktopmaschinen im Datencenter für die meisten Bereitstellungsmethoden installiert, aber er kann auch auf physischen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

PCs für Remote-PC-Zugriff installiert werden.

Der Controller besteht aus unabhängigen Windows-Diensten, die Ressourcen, Anwendungen und Desktops verwalten und die Last der Benutzerverbindungen optimieren und ausgleichen. Jede Site hat einen oder mehrere Controller. Da Sitzungen von der Latenz, Bandbreite und Netzwerkzuverlässigkeit abhängig sind, sollten alle Controller idealerweise im gleichen LAN sein.

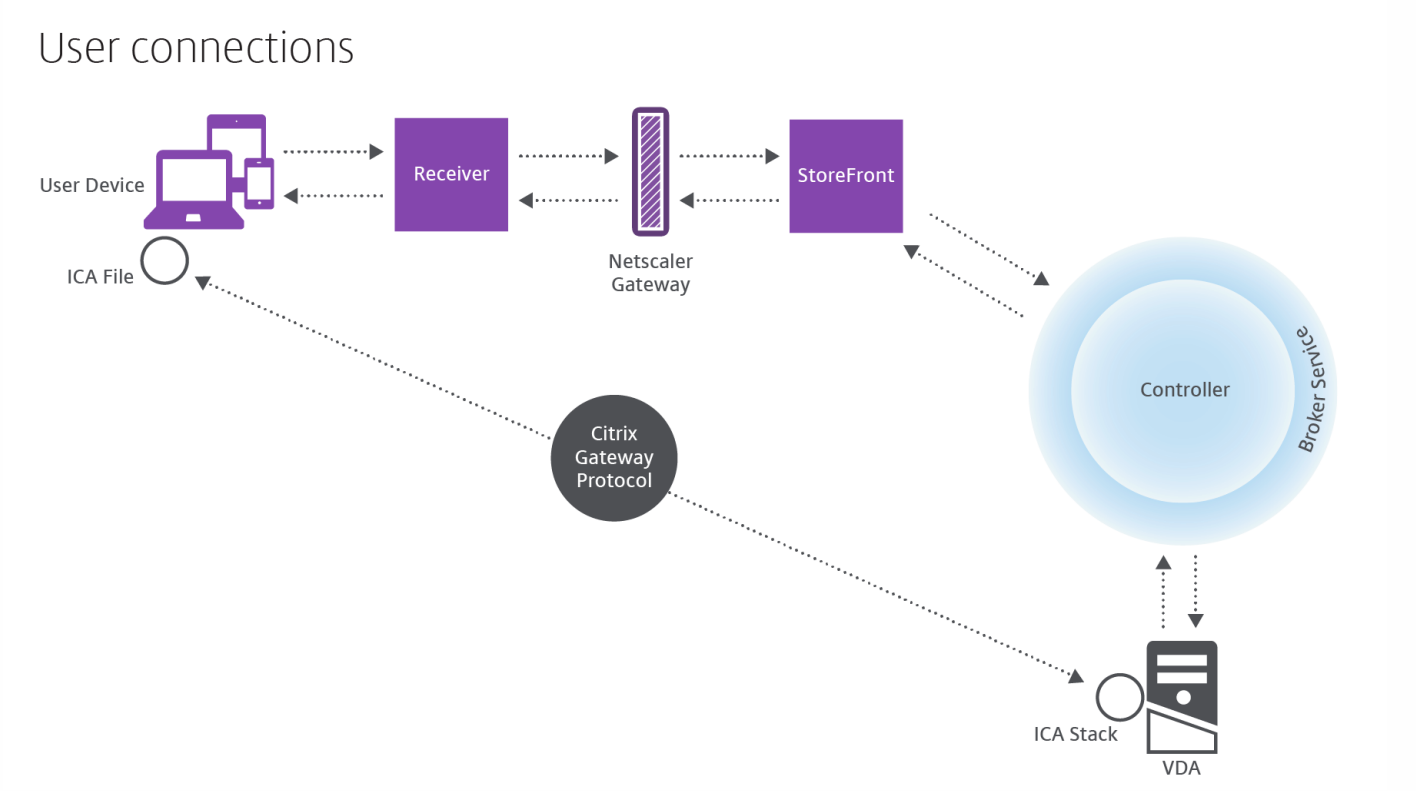
Benutzer greifen niemals direkt auf den Controller zu. Der VDA dient als Vermittler zwischen den Benutzern und dem Controller. Wenn Benutzer sich über StoreFront an der Site anmelden, werden ihre Anmeldeinformationen an den Brokerdienst weitergeleitet. Dieser ruft, basierend auf den festgelegten Richtlinien, die Profile der Benutzer und die für sie verfügbaren Ressourcen ab.

## Behandlung von Benutzerverbindungen

Zum Starten einer XenApp- oder XenDesktop-Sitzung stellt der Benutzer eine Verbindung über Citrix Receiver her (auf dem Benutzergerät installiert), oder über Citrix Receiver für Web (RFW).

In Citrix Receiver wählt der Benutzer den gewünschten physischen oder virtuellen Desktop oder die gewünschte virtuelle Anwendung.

Die Anmeldeinformationen des Benutzers werden über diesen Weg an den Controller geleitet, der durch Kommunikation mit dem Brokerdienst bestimmt, welche Ressourcen benötigt werden. Administratoren wird empfohlen, ein SSL-Zertifikat auf StoreFront zu installieren, sodass die von Receiver kommenden Anmeldeinformationen verschlüsselt werden.




Der Brokerdienst bestimmt, auf welche Desktops und Anwendungen der Benutzer zugreifen kann.

Wenn die Anmeldeinformationen geprüft wurden, werden die Informationen zu verfügbaren Apps und Desktops über die StoreFront-Citrix Receiver-Route an den Benutzer gesendet. Wenn der Benutzer Anwendungen oder Desktops aus dieser Liste auswählt, werden diese Informationen wieder an den Controller geleitet, der den richtigen VDA zum Hosten der


© 1999-2017 Citrix Systems, Inc. All rights reserved.

einzelnen Anwendungen oder Desktops bestimmt.

Der Controller sendet eine Nachricht mit den Anmeldeinformationen des Benutzers sowie alle Daten zu dem Benutzer und der Verbindung an den VDA. Der VDA akzeptiert die Verbindung und sendet die Informationen über die gleiche Route an Citrix Receiver zurück. Citrix Receiver bündelt die gesamten Informationen, die während der Sitzung generiert wurden, und erstellt eine ICA-Datei (Independent Computing Architecture) auf dem Benutzergerät, wenn Citrix Receiver lokal installiert ist, oder auf Citrix RFW, wenn der Zugriff über das Internet erfolgt. Wenn die Site ordnungsgemäß eingerichtet wurde, sind die Anmeldeinformationen während des gesamten Vorgangs verschlüsselt.

Die ICA-Datei wird auf das Benutzergerät kopiert und richtet eine direkte Verbindung zwischen dem Gerät und dem auf dem VDA ausgeführten ICA-Stack ein. Diese Verbindung umgeht die Verwaltungsinfrastruktur von Citrix Receiver, StoreFront und Controller.

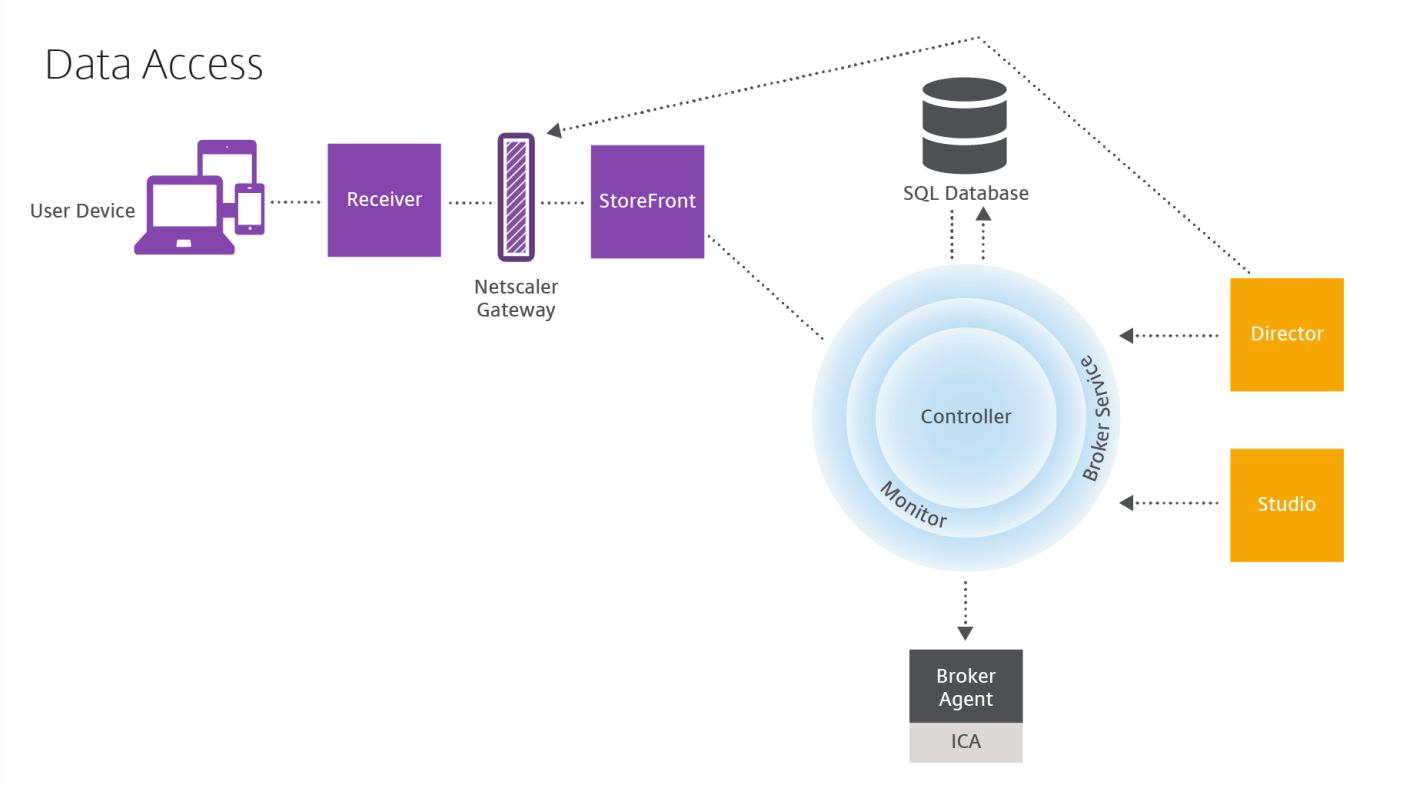
Die Verbindung zwischen Citrix Receiver und dem VDA verwendet das Citrix Gateway Protocol (CGP). Wenn eine Verbindung unterbrochen wird, kann der Benutzer bei aktivierter Sitzungszuverlässigkeit die Verbindung zum VDA wieder herstellen und muss sich nicht über die Verwaltungsinfrastruktur erneut anmelden. Die Sitzungszuverlässigkeit kann in Studio aktiviert oder deaktiviert werden.

Wenn der Client eine Verbindung zum VDA hergestellt hat, benachrichtigt der VDA den Controller, dass der Benutzer angemeldet ist, und der Controller sendet diese Informationen an die Sitedatenbank und beginnt mit der Protokollierung von Daten in der Überwachungsdatenbank.

### Funktionsweise von Datenzugriff

Jede XenApp- oder XenDesktop-Sitzung produziert Daten, auf die die IT-Mitarbeiter über Studio oder Director zugreifen können. Mit Studio können Administratoren auf Echtzeitdaten aus dem Broker Agent zugreifen und damit Sites besser verwalten. Director bietet Zugriff auf dieselben Echtzeitdaten und historischen Daten, die in der Überwachungsdatenbank gespeichert sind, sowie auf HDX-Daten von NetScaler Gateway, die dem Helpdesk zum Support und zur Problembehandlung dienen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Innerhalb des Controllers gibt der Brokerdienst Sitzungsdaten für jede Sitzung auf der virtuellen Maschine als Echtzeitdaten zurück. Der Überwachungsdienst erfasst ebenfalls die Echtzeitdaten und speichert sie als historische Daten in der Überwachungsdatenbank.

Studio kann nur mit dem Brokerdienst kommunizieren und hat daher lediglich Zugriff auf Echtzeitdaten. Director kommuniziert mit dem Brokerdienst (über ein Plug-In im Broker Agent), um auf die Sitedatenbank zuzugreifen.

Director kann zudem auf NetScaler Gateway zugreifen und Informationen zu HDX-Daten abrufen.

## Verwandter Inhalt

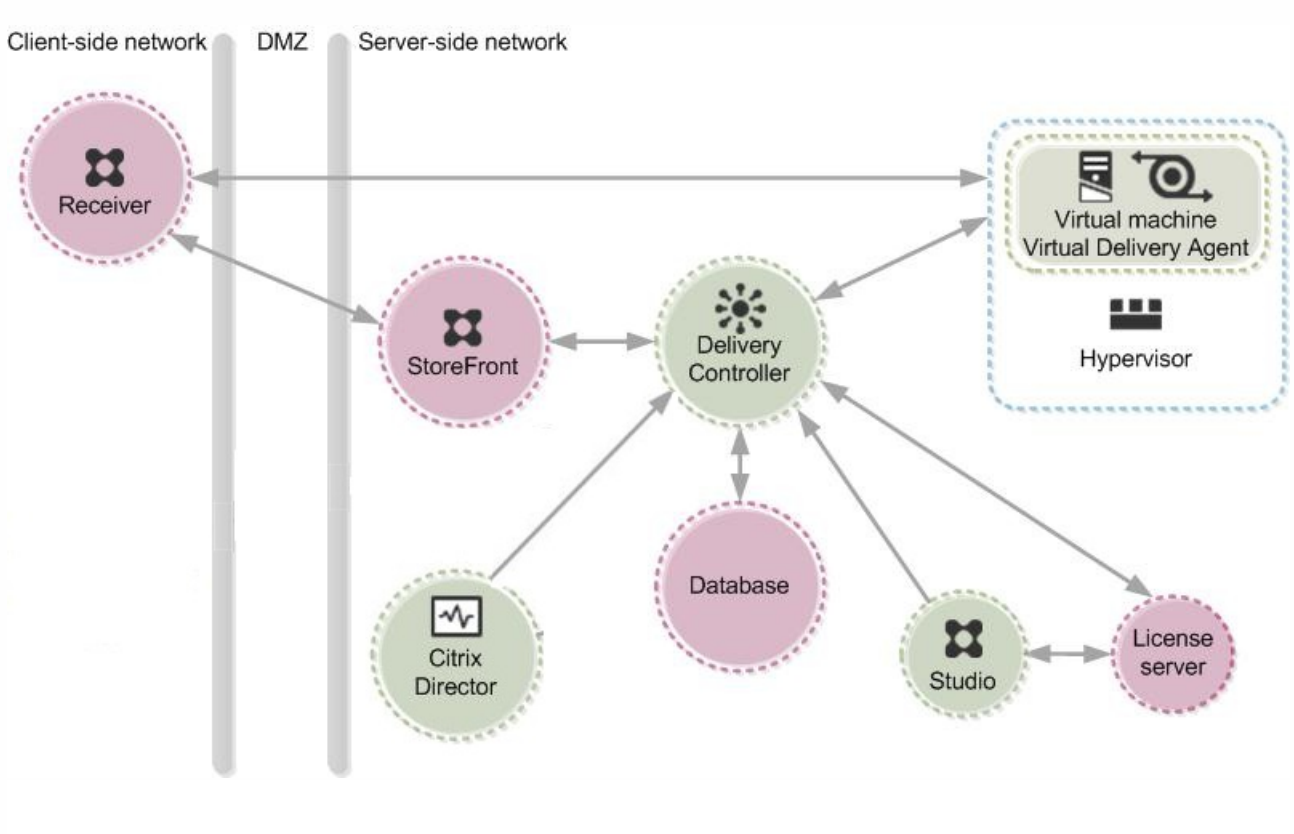
- Konzepte und Komponenten
- Bereitstellungsmethoden


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konzepte und Komponenten

Jul 08, 2016

Diese Abbildung zeigt die wichtigsten Komponenten in einer typischen XenApp- oder XenDesktop-Bereitstellung, die als *Site* bezeichnet wird.




Die Abbildung enthält folgende Komponenten:

- **Delivery Controller**: Der Delivery Controller ist die zentrale Verwaltungskomponente einer XenApp- oder XenDesktop-Site. Jede Site hat einen oder mehrere Delivery Controller. Er muss auf mindestens einem Server im Datencenter installiert sein. (Um die Zuverlässigkeit und Verfügbarkeit der Site zu gewährleisten, installieren Sie den Controller auf mehreren Servern.) Wenn Ihre Bereitstellung virtuelle Maschinen auf einem Hypervisor oder in einem Clouddienst enthält, kommunizieren die Controller-Dienste mit dem Hypervisor, um Anwendungen und Desktops zu verteilen, den Benutzerzugriff zu authentifizieren und zu verwalten, Verbindungen zwischen Benutzern und ihren virtuellen Desktops und Anwendungen zu vermitteln, Benutzerverbindungen zu optimieren und einen Lastausgleich für die Verbindungen auszuführen.
  Die Daten dieser Dienste werden in der Sitedatenbank gespeichert.

  Der Controller verwaltet den Zustand der Desktops, startet und hält sie basierend auf dem Bedarf und der administrativen Konfiguration an. In bestimmten Editionen ermöglicht der Controller die Installation der Profilverwaltung, mit der Sie personalisierte Einstellungen in virtualisierten oder physischen Windows-Umgebungen verwalten.

- **Datenbank**: Mindestens eine Microsoft SQL Server-Datenbank ist pro XenApp- oder XenDesktop-Site zum Speichern der Konfigurations- und Sitzungsinformationen erforderlich. Diese Datenbank speichert die Daten, die von den Diensten des Controllers gesammelt und verwaltet werden. Installieren Sie die Datenbank in Ihrem Datencenter und stellen Sie eine persistente Verbindung mit dem Controller sicher.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Virtual Delivery Agent (VDA)**: Der VDA ist auf jeder physischen oder virtuellen Maschine der Site installiert, die Sie Benutzern zur Verfügung stellen möchten. Durch ihn kann sich die Maschine beim Controller registrieren, sodass die Maschine und die darauf gehosteten Ressourcen Benutzern verfügbar gemacht werden können. VDAs erstellen und verwalten die Verbindung zwischen der Maschine und dem Benutzergerät, prüfen, ob eine Citrix Lizenz für den Benutzer oder die Sitzung verfügbar ist und wenden die für die Sitzung konfigurierten Richtlinien an. Der VDA übermittelt über den Broker Agent Sitzungsinformationen an den Brokerdienst auf dem Controller.
  VDAs sind für Windows-Serverbetriebssysteme und Windows-Desktopbetriebssysteme verfügbar. Mit VDAs für Windows-Serverbetriebssysteme können mehrere Benutzer gleichzeitig eine Verbindung mit dem Server herstellen. Mit VDAs für Windows-Desktopbetriebssysteme kann jeweils nur ein Benutzer eine Verbindung zum Desktop herstellen.

- **Citrix StoreFront:** dient zur Authentifizierung von Benutzern für Sites mit Ressourcen und zur Verwaltung von Stores mit Desktops und Anwendungen für die Benutzer. StoreFront hostet den Unternehmensanwendungsstore, über den Sie Benutzern Self-Service-Zugriff auf Desktops und Anwendungen gewähren, die Sie verfügbar machen. Außerdem verfolgt es die Anwendungsabonnements von Benutzern sowie Verknüpfungsnamen und andere Daten, um eine konsistente Benutzererfahrung über mehrere Geräte sicherzustellen.
- **Citrix Receiver:** wird auf Benutzergeräten und anderen Endpunkten installiert, u. a. virtuellen Desktops, und bietet Benutzern schnellen, sicheren Self-Service-Zugriff auf Dokumente, Anwendungen und Desktops von allen Geräten (Smartphones, Tablets, PCs) aus. Citrix Receiver bietet bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen. Bei Geräten, auf denen die Citrix Receiver-Software nicht installiert werden kann, ermöglicht Citrix Receiver für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.
- **Citrix Studio**: Dies ist die Verwaltungskonsole, mit der Sie die Bereitstellung konfigurieren und verwalten, wobei keine separaten Verwaltungskonsolen für die Bereitstellung von Anwendungen und Desktops benötigt werden. Studio bietet zahlreiche Assistenten, die Ihnen bei der Einrichtung Ihrer Umgebung, dem Erstellen der Arbeitslast zum Hosten von Anwendungen und Desktops sowie beim Zuweisen von Anwendungen und Desktops zu Benutzern behilflich sind. Sie können mit Studio auch Citrix Lizenzen für die Site zuweisen und verfolgen.
  Studio erhält die Informationen, die es anzeigt, vom Brokerdienst auf dem Controller.

- **Citrix Director**: Director ist ein webbasiertes Tool, mit dem die Support- und Helpdesk-Teams eine XenDesktop-Umgebung überwachen, potenziell systembedrohende Probleme rechtzeitig behandeln und Unterstützung für Endbenutzer leisten können. Sie können eine Director-Bereitstellung zur Verbindungen mit und Überwachung von mehreren XenApp- bzw. XenDesktop-Sites verwenden. In Director werden folgende Sitzungs- und Siteinformationen angezeigt:

  - Echtzeit-Sitzungsdaten vom Brokerdienst auf dem Controller, einschließlich Daten, die der Brokerdienst vom Broker Agent auf dem VDA erhält.
  - Historische Daten für die Site vom Überwachungsdienst auf dem Controller.
  - Daten zum HDX-Datenverkehr (auch ICA-Datenverkehr genannt), die von HDX Insight auf dem NetScaler erfasst werden, wenn die Bereitstellung einen NetScaler und die XenApp- oder XenDesktop-Edition HDX Insights enthält.

  Zudem können Sie über Microsoft-Remoteunterstützung auch Benutzersitzungen anzeigen und steuern.

- **Citrix Lizenzserver**: Der Lizenzserver verwaltet die Produktlizenzen. Er kommuniziert mit dem Controller, um die Lizenzierung jeder Benutzersitzung zu verwalten, und mit Studio, um Lizenzdateien zuzuteilen. Sie müssen mindestens einen Lizenzserver zum Speichern und Verwalten Ihrer Lizenzdateien erstellen.
- **Hypervisor**: Der Hypervisor hostet die virtuellen Maschinen in der Site. Dies können virtuellen Maschinen sein, die Sie zum


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hosten von Anwendungen und Desktops verwenden, und auch virtuellen Maschinen, die Sie zum Hosten von XenApp- und XenDesktop-Komponenten verwenden. Ein Hypervisor wird auf einem Hostcomputer installiert, der nur zur Ausführung des Hypervisors und dem Hosten virtueller Maschinen bestimmt ist.
Der Citrix XenServer-Hypervisor ist in XenApp und XenDesktop enthalten. Sie können auch andere unterstützte Hypervisors verwenden, z. B. Microsoft Hyper-V oder VMware vSphere.

Obwohl für viele Implementierungen von XenApp und XenDesktop ein Hypervisor erforderlich ist, benötigen Sie keinen für Remote-PC-Zugriff oder wenn Sie Provisioning Services statt MCS zum Bereitstellen von virtuellen Maschinen verwenden. Provisioning Services ist in bestimmten XenApp-/XenDesktop-Editionen enthalten.

Diese zusätzlichen Komponenten, die nicht in der Abbildung oben enthalten sind, können auch in typischen XenApp- oder XenDesktop-Bereitstellungen enthalten sein:

- **Provisioning Services**: Provisioning Services ist eine optionale Komponente von XenApp und XenDesktop und steht in einigen Editionen zur Verfügung. Es bietet eine Alternative zu MCS für das Provisioning von virtuellen Maschinen. Während MCS Kopien eines Masterimages erstellt, streamt Provisioning Services das Masterimage zum Benutzergerät. Provisioning Services benötigen hierfür keinen Hypervisor, daher können Sie mit Provisioning Services physische Maschinen hosten. Wenn Provisioning Services in einer Site installiert ist, kommuniziert es mit dem Controller, um Benutzern Ressourcen bereitzustellen.
- **NetScaler Gateway**: Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in diesem Release mit Citrix NetScaler Gateway (früher Access Gateway) mit TLS gesichert werden. NetScaler Gateway oder NetScaler VPX virtuelles Gerät ist ein SSL-VPN-Gerät, das in der DMZ (demilitarisierten Zone) bereitgestellt wird und sicheren, zentralen Zugriff über die Unternehmensfirewall bietet.
- **Citrix CloudBridge**: In Bereitstellungen, in denen virtuelle Desktops den Benutzern an Remotestandorten wie etwa Zweigstellen bereitgestellt werden, kann mit Citrix CloudBridge (früher Citrix Branch Repeater oder WANScaler) die Leistung optimiert werden. Repeater erhöhen die Leistung in WAN-Netzwerken. Mit Repeatern im Netzwerk erleben Benutzer in Zweigstellen eine LAN-ähnliche Leistung über das WAN. CloudBridge kann bestimmten Teilen der Benutzererfahrung Priorität geben, damit sich beispielsweise die Benutzererfahrung in der Zweigstelle nicht verschlechtert, wenn eine große Datei oder ein großer Druckauftrag über das Netz gesendet wird. HDX WAN-Optimierung mit CloudBridge bietet Komprimierung mit Token sowie Entfernung von Datenduplikaten, wodurch die Bandbreitenanforderungen drastisch reduziert werden und die Leistung verbessert wird. Weitere Informationen finden Sie in der Dokumentation für Citrix CloudBridge.

# Einrichten und Zuweisen von Ressourcen: Maschinenkataloge und Bereitstellungsgruppen

Sie richten die Ressourcen, die Sie Benutzern bereitstellen möchten, mit Maschinenkatalogen ein; welche Benutzer Zugriff auf diese Ressourcen haben, wird mit Bereitstellungsgruppen festgelegt.

**Maschinenkataloge**

Maschinenkataloge sind Sammlungen virtueller oder physischer Maschinen, die Sie als Einheit verwalten. Diese Maschinen und die Anwendungen oder virtuellen Desktops darauf sind die Ressourcen, die Sie den Benutzer bereitstellen. Auf allen Maschinen in einem Maschinenkatalog ist das gleiche Betriebssystem und der gleiche Virtual Desktop Agent (VDA) installiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sie verfügen auch über dieselben Anwendungen oder virtuellen Desktops. Normalerweise erstellen Sie ein Masterimage und verwenden es zum Erstellen identischer virtueller Maschinen im Maschinenkatalog. Beim Erstellen eines Maschinenkatalogs geben Sie den Typ und die Bereitstellungsmethode für die Maschinen in dem Katalog an.

- **Serverbetriebssystemmaschinen**: virtuelle oder physische Maschinen, die auf einem Serverbetriebssystem basieren und dazu verwendet werden, mit XenApp veröffentlichte Apps (serverbasierte, gehostete Anwendungen) und mit XenApp veröffentlichte Desktops (servergehostete Desktops) bereitstellen. Mehrere Benutzer können gleichzeitig eine Verbindung mit diesen Maschinen herstellen.
- **Desktopbetriebssystemmaschinen**: virtuelle oder physische Maschinen, die auf einem Desktopbetriebssystem basieren und die VDI-Desktops (Desktops, auf denen Desktopbetriebssysteme ausgeführt werden, die abhängig von den ausgewählten Optionen vollständig personalisiert werden können), VM-gehostete Apps (Anwendungen von Desktopbetriebssystemen) und gehostete physische Desktops bereitstellen. Nur jeweils ein Benutzer kann eine Verbindung zu einem dieser Desktops herstellen.
- **Remote-PC-Zugriff**: Wenn Benutzergeräte auf einer Positivliste enthalten sind, können die Benutzer von einem beliebigen Gerät aus, auf dem Citrix Receiver ausgeführt wird, auf ihre Büro-PCs zugreifen. Remote-PC-Zugriff ermöglicht das Verwalten des Zugriffs auf Büro-PCs über die XenDesktop-Bereitstellung.

**Provisioningmethoden**

- **Maschinenerstellungsdienste (MCS)**: Sammlung von Diensten, die bei Bedarf virtuelle Server und Desktops von einem Masterimage erstellen, die Speichernutzung optimieren und den Benutzern bei jeder Anmeldung eine virtuelle Maschine bereitstellen. MCS ist vollständig in Citrix Studio integriert und wird dort verwaltet.
- **Provisioning Services**: ermöglicht Provisioning und erneutes Provisioning von Computern in Echtzeit von einem freigegebenen Datenträgerimage. Zielgeräte werden von Provisioning Services als eine Gerätesammlung verwaltet. Die Desktops und Anwendungen werden von einer Provisioning Services-vDisk bereitgestellt, deren Image von einem Masterzielgerät erstellt wurde. So können Sie die Verarbeitungsleistung der physischen Hardware oder der virtuellen Maschinen nutzen. Provisioning Services werden in einer eigenen Konsole verwaltet.
- **Vorhandene Images**: bezieht sich auf Desktops und Anwendungen, die Sie bereits auf virtuelle Maschinen im Datencenter migriert haben. Sie müssen die Zielgeräte individuell oder kollektiv mit ESD-Tools (Electronic Software Distribution) verwalten.

**Bereitstellungsgruppen**

Bereitstellungsgruppen sind Sammlungen von Benutzern, denen Zugriff auf eine gemeinsame Gruppe von Ressourcen erteilt wird. Bereitstellungsgruppen enthalten Maschinen von Ihren Maschinenkatalogen und Active Directory-Benutzer, die Zugriff auf die Site haben. Oft ist es sinnvoll, Benutzer den Bereitstellungsgruppen nach ihrer Active Directory-Gruppe zuzuweisen, da sowohl Active Directory-Gruppen als auch Bereitstellungsgruppen Methoden sind, um Benutzer mit ähnlichen Anforderungen zu gruppieren. Jede Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen enthalten und jeder Maschinenkatalog kann Maschinen für mehrere Bereitstellungsgruppen beitragen, aber eine Maschine kann jeweils nur zu einer Bereitstellungsgruppe gehören. Sie können Bereitstellungsgruppen für Anwendungen, Desktops oder beides einrichten. Dabei definieren Sie, auf welche Ressourcen Benutzer in der Bereitstellungsgruppe zugreifen können. Beispiel: Sie möchten verschiedene Anwendungen verschiedenen Benutzern bereitstellen. Eine Methode ist die Installation aller bereitzustellenden Anwendungen auf dem Masterimage für einen Maschinenkatalog. Dann erstellen Sie in diesem Katalog genug Maschinen, um sie auf mehrere Bereitstellungsgruppen zu verteilen. Anschließend konfigurieren Sie jede Bereitstellungsgruppe so, dass sie einen anderen Teil der auf den Maschinen installierten Anwendungen bereitstellt.

# Unterschiede zwischen XenApp und XenDesktop 7.x


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# und XenApp-Versionen bis 6.5

Wenn Sie mit XenApp 6.5 und Vorversionen vertraut sind, kann es nützlich sein, sich die Unterschiede zwischen XenApp und XenDesktop 7.x und diesen älteren Versionen anzuschauen.

> **Hinweis:** In diesem Abschnitt bezieht sich die Angabe 7.x auf XenApp ab Version 7.5 und auf XenDesktop ab Version 7.

Obwohl die funktionellen Elemente nicht genau gleich sind, erleichtert die folgende Tabelle das Zuordnen der funktionellen Elemente von XenApp bis Version 6.5 zu jenen von XenApp und XenDesktop 7.x:

| XenApp 6.5 und Vorversionen | XenApp und XenDesktop 7.x |
|---|---|
| Independent Management Architecture (IMA) | FlexCast Management Architecture (FMA) |
| Farm | Site |
| Workergruppe | Maschinenkatalog<br><br>Bereitstellungsgruppe |
| Worker | Virtual Delivery Agent (VDA)<br><br>Serverbetriebssystemmaschine, VDA für Serverbetriebssystem<br><br>Desktopbetriebssystemmaschine, VDA für Desktopbetriebssystem |
| Remotedesktopdienste (RDS) oder Terminaldienste-Maschine | Serverbetriebssystemmaschine, VDA für Serverbetriebssystem |
| Zonen- und Datensammelpunkt | Delivery Controller |
| Delivery Services Console | Citrix Studio und Citrix Director |
| Veröffentlichen von Anwendungen | Bereitstellen von Anwendungen |
| Datenspeicher | Datenbank |
| Lastauswertungsprogramm | Lastverwaltungsrichtlinie |
| Administrator | Delegierter Administrator |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | Rolle<br><br>Geltungsbereich |

XenApp und XenDesktop 7.x basieren auf der FlexCast Management Architecture (FMA). Die FMA ist eine dienstorientierte Architektur, die über Citrix Technologien übergreifend Interoperabilität und Verwaltungsmodularität ermöglicht Die FMA bietet eine Plattform für die Anwendungsbereitstellung, Mobilität, Dienste, flexible Bereitstellung und Cloudverwaltung.

Die FMA ersetzt die Independent Management Architecture (IMA) in XenApp 6.5 und Vorversionen.

Dies sind die Hauptelemente der FMA gegenüber den Elementen von XenApp 6.5 und Vorversionen:

- **Bereitstellungssites:** Farmen waren die Objekte der obersten Ebene in XenApp 6.5 und Vorversionen. In XenApp und XenDesktop 7.x ist dies die Site. Über Sites werden Benutzergruppen Anwendungen und Desktops angeboten. Die FMA erfordert, dass Sie in einer Domäne sind, um eine Site bereitzustellen. Beispiel: Zum Installieren der Server muss Ihr Konto lokale Administratorrechte haben und in Active Directory ein Domänenbenutzer sein.
- **Maschinenkataloge und Bereitstellungsgruppen:** Maschinen, auf denen Anwendungen gehostet werden, gehörten in XenApp 6.5 und Vorversionen zu Workergruppen, um eine effiziente Verwaltung von Anwendungen und Serversoftware zu ermöglichen. Administratoren konnten für die Anwendungsverwaltung und für den Lastausgleich alle Maschinen in einer Workergruppe als eine Einheit behandeln. Ordner wurden verwendet, um Anwendungen und Maschinen zu organisieren. In XenApp und XenDesktop 7.x verwenden Sie eine Kombination aus Maschinenkatalogen und Bereitstellungsgruppen, um Maschinen, den Lastausgleich und gehostete Anwendungen oder Desktops zu verwalten. Sie können auch Anwendungsordner verwenden.
- **Virtual Delivery Agents (VDAs):** In XenApp 6.5 und Vorversionen wurden auf Maschinen in Workergruppen Anwendungen für die Benutzer ausgeführt und die Maschinen kommunizierten mit Datensammelpunkten. In XenApp und XenDesktop 7.x kommuniziert der VDA mit Delivery Controllern, die die Benutzerverbindungen verwalten.
- **Delivery Controller:** In XenApp 6.5 und Vorversionen war ein Zonenmaster für Verbindungsanfragen von Benutzern und die Kommunikation mit Hypervisors zuständig. In XenApp und XenDesktop 7.x verteilen und handhaben Controller in der Site Verbindungsanfragen. In XenApp 6.5 und Vorversionen ermöglichten Zonen das Aggregieren von Servern und Replizieren von Daten über WAN-Verbindungen. Die Zonen in XenApp und XenDesktop 7.x sind zwar keine exakte Entsprechung, dennoch können Sie mit ihnen Benutzern an entfernten Standorten eine Verbindung mit Ressourcen ermöglichen, ohne dass diese große WAN-Segmente durchqueren muss.
- **Citrix Studio und Citrix Director:** Mit der Studio-Konsole können Sie Umgebungen konfigurieren und Benutzern Zugriff auf Anwendungen und Desktops gewähren. Studio ersetzt die Delivery Services Console in XenApp 6.5 und Vorversionen. Administratoren verwenden Director, um die Umgebung zu überwachen, Benutzergeräte zu spiegeln und IT-Probleme zu behandeln. Zum Spiegeln von Benutzern muss die Microsoft-Remoteunterstützung aktiviert sein; sie ist standardmäßig aktiviert, wenn der VDA installiert ist.
- **Anwendungsbereitstellung:** In XenApp 6.5 und Vorversionen wurden mit dem Assistenten zur Anwendungsveröffentlichung Anwendungen vorbereitet und für Benutzer bereitgestellt. In XenApp und XenDesktop 7.x erstellen Sie Anwendungen mit Studio und stellen Sie den Benutzern in einer Bereitstellungsgruppe zur Verfügung. In Studio konfigurieren Sie zunächst eine Site, erstellen und geben Maschinenkataloge an und dann erstellen Sie Bereitstellungsgruppen, die Maschinen aus diesen Maschinenkatalogen verwenden. Mit Bereitstellungsgruppen wird festgelegt, welche Benutzer Zugriff auf die bereitgestellten Anwendungen haben.
- **Datenbank:** In XenApp und XenDesktop 7.x werden die Konfigurationsinformationen nicht im IMA-Datenspeicher gespeichert. Stattdessen werden Konfigurations- und Sitzungsinformationen in einer Microsoft SQL Server-Datenbank gespeichert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Lastverwaltungsrichtlinie:** In XenApp 6.5 und Vorversionen verwenden Lastauswertungsprogramme vordefinierte Messungen zur Bestimmung der Last auf einer Maschine. Benutzerverbindungen können weniger ausgelasteten Maschinen zugeordnet werden. In XenApp und XenDesktop 7.x erfolgt der Lastausgleich auf Maschinen mit Lastverwaltungsrichtlinien.
- **Delegierte Administration:** In XenApp 6.5 und Vorversionen wurden benutzerdefinierte Administratoren erstellt und ihnen wurden Berechtigungen auf der Basis von Ordnern und Objekten zugewiesen. In XenApp und XenDesktop 7.x basieren benutzerdefinierte Administratoren auf Rollen- und Geltungsbereichspaaren. Eine Rolle repräsentiert eine Stellenfunktion. Ihr sind definierte Berechtigungen zugewiesen, die eine Delegierung erlauben. Ein Geltungsbereich steht für eine Sammlung von Objekten. Vordefinierte Administratorrollen haben spezifische Berechtigungssätze, z. B. für Helpdesk, Anwendungen, Hosting und Kataloge. Beispiel: Helpdeskadministratoren können nur mit einzelnen Benutzern in bestimmten Sites arbeiten, während Volladministratoren die gesamte Bereitstellung überwachen und systemweite IT-Probleme behandeln können.

Der Übergang zu FMA bedeutet außerdem, dass einige in XenApp 6.5 und Vorversionen verwendete Features möglicherweise anders implementiert worden sind oder dass Sie sie eventuell durch andere Features, Komponenten oder Tools ersetzen müssen, um das gleiche Ziel zu erreichen.

| XenApp 6.5 und Vorversionen | XenApp und XenDesktop 7.x |
|---|---|
| Sitzungsvorabstart und Sitzungsfortbestehen, die mit Richtlinieneinstellungen konfiguriert sind | Sitzungsvorabstart und Sitzungsfortbestehen, die durch Bearbeiten der Bereitstellungsgruppeneinstellungen konfiguriert sind.<br><br>Wie in XenApp 6.5 ermöglichen diese Features Benutzern einen schnellen Zugriff auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden (Sitzungsvorabstart), und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat (Sitzungsfortbestehen). In XenApp und XenDesktop 7.x aktivieren Sie die Features für bestimmte Benutzer, indem Sie diese Einstellungen für vorhandene Bereitstellungsgruppen konfigurieren. Siehe Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen. |
| Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Zuweisen von Rechten für anonyme Benutzer beim Festlegen der Eigenschaften für veröffentlichte Anwendungen | Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Konfigurieren dieser Option, wenn Sie die Benutzereigenschaften einer Bereitstellungsgruppe festlegen. Siehe Benutzer. |
| Lokaler Hostcache ermöglicht das Funktionieren eines Workerservers, selbst wenn eine Verbindung zum Datenspeicher nicht verfügbar ist | Verbindungsleasing ermöglicht Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops, selbst wenn die Sitedatenbank nicht verfügbar ist. Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zum Bereitstellen hoher Verfügbarkeit bei SQL Server. Siehe Verbindungsleasing. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Anwendungsstreaming | App-V stellt gestreamte Anwendungen bereit, die mit Studio verwaltet werden. |
| Webinterface | Citrix empfiehlt, dass Sie StoreFront einsetzen. |
| SmartAuditor | Verwenden Sie die Sitzungsaufzeichnung. Sie können auch alle Sitzungsaktivitäten aus einer administrativen Perspektive mit der Konfigurationsprotokollierung aufzeichnen. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Active Directory

Jul 08, 2016

Active Directory ist zum Authentifizieren und Autorisieren erforderlich. Mit der Kerberos-Infrastruktur in Active Directory wird die Authentizität und Vertraulichkeit der Kommunikation zwischen den Delivery Controllern garantiert. Informationen zu Kerberos finden Sie in der Dokumentation von Microsoft.

Der Artikel Systemanforderungen enthält die unterstützten Funktionsebenen für Gesamtstruktur und Domäne. Zur Verwendung der Richtlinienmodellierung muss der Controller unter Windows 2003 oder höher bis Windows Server 2012 R2 ausgeführt werden. Dies wirkt sich nicht auf die Domänenfunktionsebene aus.

Dieses Produkt unterstützt Folgendes:

- Bereitstellungen, in denen die Benutzerkonten und Computerkonten in Domänen in einer einzigen Active Directory-Gesamtstruktur bestehen. Benutzer- und Computerkonten können in beliebigen Domänen in einer Gesamtstruktur bestehen. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- Bereitstellungen, in denen die Benutzerkonten und die Computerkonten der Controller und virtuellen Desktops in unterschiedlichen Active Directory-Gesamtstrukturen bestehen. Bei diesem Bereitstellungstyp muss eine Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und virtuellen Desktops und den Domänen mit den Benutzerkonten bestehen. Sie können Gesamtstruktur- oder externe Vertrauensstellungen verwenden. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- Bereitstellungen, in denen die Computerkonten für Controller in einer Active Directory-Gesamtstruktur bestehen, die sich von den zusätzlichen Active Directory-Gesamtstrukturen mit den Computerkonten für die virtuellen Desktops unterscheidet. Bei diesem Bereitstellungstyp muss eine bidirektionale Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und allen Domänen mit den Computerkonten der virtuellen Desktops bestehen. Bei diesem Bereitstellungstyp müssen alle Domänen mit Computerkonten für Controller oder virtuelle Desktops mindestens auf der Funktionsebene "Windows 2000 native" sein. Alle Funktionsebenen der Gesamtstruktur werden unterstützt.
- Beschreibbarer Domänencontroller. Schreibgeschützte Domänencontroller werden nicht unterstützt.

Virtual Delivery Agents (VDAs) können mit in Active Directory veröffentlichten Informationen die Contoller ermitteln, bei denen sie sich registrieren können (Discovery). Diese Methode wird primär für Abwärtskompatibilität unterstützt und ist nur verfügbar, wenn die VDAs und die Controller in derselben Active Directory-Gesamtstruktur sind. Weitere Informationen zu dieser Ermittlungsmethode finden Sie im Artikel Delivery Controller und unter CTX118976.

**Tipp:** Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers, nachdem Sie die Site konfiguriert haben.

## Bereitstellen in einer Active Directory-Umgebung mit mehreren Gesamtstrukturen

Hinweis: Diese Informationen gelten für Versionen ab XenDesktop 7.1 und XenApp 7.5. Sie gelten nicht für ältere Versionen von XenDesktop und XenApp.
Bei einer Active Directory-Umgebung mit mehreren Gesamtstrukturen und unidirektionalen oder bidirektionalen Vertrauensstellungen können Sie DNS-Weiterleitungen zur Suche und Registrierung von Namen verwenden. Mit dem Assistenten zum Zuweisen der Objektverwaltung können Sie den entsprechenden Active Directory-Benutzern das Erstellen von Computerkonten ermöglichen. Weitere Informationen zu diesem Assistenten finden Sie in der Dokumentation von Microsoft.

In der DNS-Infrastruktur sind keine Reverse-DNS-Zonen erforderlich, wenn die entsprechenden DNS-Weiterleitungen zwischen Gesamtstrukturen eingerichtet sind.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Der SupportMultipleForest-Schlüssel ist erforderlich, wenn der VDA und der Controller in unterschiedlichen Gesamtstrukturen eingerichtet sind, unabhängig davon, ob sich die Active Directory- und NetBIOS-Namen voneinander unterscheiden. Der Schlüssel "SupportMultipleForest" ist nur auf dem VDA nötig. Mit den folgenden Informationen fügen Sie einen Registrierungsschlüssel hinzu:
**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Name: SupportMultipleForest
  - Typ: REG_DWORD
  - Wert: 0x00000001 (1)

Sie müssen möglicherweise die DNS-Konfiguration umkehren, wenn sich der DNS-Namespace vom Active Directory-Namespace unterscheidet.

Wenn externe Vertrauensstellungen während des Setups vorhanden sind, ist der Registrierungsschlüssel "ListOfSIDs" erforderlich. Der Registrierungsschlüssel "ListOfSIDs" ist auch erforderlich, wenn der vollqualifizierte Domänenname (FQDN) für Active Directory sich vom DNS-FQDN unterscheidet oder die Domäne mit dem Domänencontroller einen anderen Netbios-Namen hat als der Active Directory-FQDN. Verwenden Sie zum Hinzufügen des Registrierungsschlüssels die folgenden Informationen:

- Für einen 32-Bit- oder 64-Bit-VDA verwenden Sie den Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs.
  - Name: ListOfSIDs
  - Typ: REG_SZ
  - Daten: Sicherheits-ID (SID) der Controller

Wenn externe Vertrauensstellungen vorhanden sind, nehmen Sie die folgenden Änderungen auf dem VDA vor:

1. Navigieren Sie zur Datei: \Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config.
2. Erstellen Sie eine Sicherungskopie der Datei.
3. Öffnen Sie die Datei in einem Textbearbeitungsprogramm, z. B. Editor.
4. Suchen Sie den Text allowNtlm="false" und ändern Sie den Text in allowNtlm="true".
5. Speichern Sie die Datei.

Nach dem Hinzufügen des Registrierungsschlüssels "ListOfSIDs" und der Bearbeitung der Datei brokeragent.exe.config starten Sie den Citrix Desktopdienst neu, um die Änderungen anzuwenden.

In der folgenden Tabelle werden die unterstützten Vertrauenstypen aufgeführt:

| Vertrauenstyp | Transitivität | Richtung | In diesem Release unterstützt |
|---|---|---|---|
| Über-/untergeordnet | Transitiv | Bidirektional | Ja |
| Strukturstamm | Transitiv | Bidirektional | Ja |
| Externe Schicht | Nicht transitiv | Unidirektional oder bidirektional | Ja |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Vertrauenstyp | Transitivität | Richtung | In diesem Release unterstützt |
|---|---|---|---|
| Gesamtstruktur | Transitiv | Unidirektional oder bidirektional | Ja |
| Shortcut | Transitiv | Unidirektional oder bidirektional | Ja |
| Bereich | Transitiv oder nicht transitiv | Unidirektional oder bidirektional | Nein |

Weitere Informationen über komplexe Active Directory-Umgebungen finden Sie unter CTX134971.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Datenbanken

Jul 15, 2016

XenApp- bzw. XenDesktop-Sites verwenden drei SQL Server-Datenbanken:

- **Site:** (auch "Sitekonfiguration") enthält die Konfiguration der ausgeführten Site sowie den aktuellen Sitzungszustand und Verbindungsinformationen.
- **Konfigurationsprotokollierung**: (auch "Protokollierung") enthält Informationen über Änderungen an der Sitekonfiguration und Administratoraktivitäten. Diese Datenbank wird verwendet, wenn die Konfigurationsprotokollierung aktiviert ist (diese ist standardmäßig aktiviert).
- **Überwachung:** enthält von Director genutzte Daten, z. B. Sitzungs- und Verbindungsinformationen.

Jeder Delivery Controller kommuniziert mit der Sitedatenbank, zwischen Controller und Datenbank ist eine Windows-Authentifizierung erforderlich. Ein Controller kann entfernt oder ausgeschaltet werden, ohne dass dies Auswirkungen auf die anderen Controller in der Site hat. Das bedeutet jedoch, dass die Datenbank einen zentralen Ausfallpunkt bildet. Wenn der Datenbankserver ausfällt, funktionieren vorhandene Verbindungen weiterhin, bis der Benutzer sich abmeldet oder die Verbindung trennt. Neue Verbindungen können nicht hergestellt werden, wenn der Datenbankserver nicht verfügbar ist, außer in manchen Fällen, wenn das Verbindungsleasing konfiguriert ist.

Citrix empfiehlt, dass Sie regelmäßig ein Backup der Datenbanken durchführen, damit diese bei einem Ausfall des Datenbankservers von dem Backup wiederhergestellt werden können. Die Backupstrategie kann für jede Datenbank anders sein. Anweisung finden Sie unter CTX135207.

Wenn die Site mehr als eine Zone enthält, muss die Sitedatenbank in der primären Zone residieren. Controller in jeder Zone kommunizieren mit der Datenbank.

# Hohe Verfügbarkeit

Es gibt einige Hochverfügbarkeitslösungen, die Sie in Betracht ziehen können, um automatisches Failover zu gewährleisten:

- **AlwaysOn-Verfügbarkeitsgruppen:** Dies ist eine Lösung für Hochverfügbarkeit und Notfallwiederherstellung, die mit SQL Server 2012 eingeführt wurde. Damit können Sie die Verfügbarkeit für eine oder mehrere Datenbanken maximieren. AlwaysOn-Verfügbarkeitsgruppen erfordern, dass die SQL Server-Instanzen auf Windows Server Failover Clustering-Knoten (WSFC) residieren. Weitere Informationen finden Sie unter http://msdn.microsoft.com/en-us/library/hh510230.
- **Spiegelung der SQL Server-Datenbank:** Dies stellt sicher, dass ein automatischer Failoverprozess in nur wenigen Sekunden stattfindet, falls der aktive Datenbankserver ausfällt. Benutzer werden in der Regel also nicht beeinträchtigt. Diese Methode ist teurer als andere Lösungen, da Volllizenzen für SQL Server auf jedem Datenbankserver erforderlich sind. In gespiegelten Umgebungen kann SQL Server Express nicht verwendet werden.
- **SQL-Clustering:** Mit dieser Technologie von Microsoft können Sie einem Server automatisch erlauben, die Aufgaben und Verantwortlichkeiten eines anderen, fehlgeschlagenen Servers zu übernehmen. Es ist jedoch etwas komplizierter, diese Lösung einzurichten. Zudem ist der automatische Failoverprozess in der Regel langsamer als bei anderen Lösungen (etwa der SQL-Spiegelung).
- **Verwenden der Hochverfügbarkeitsfeatures des Hypervisors:** Bei dieser Methode wird die Datenbank als eine virtuelle Maschine bereitgestellt und die Hochverfügbarkeitsfeatures des Hypervisors werden verwendet. Diese Lösung ist billiger als das Spiegeln, da die bestehende Hypervisorsoftware verwendet wird und Sie zudem SQL Server Express verwenden können. Der automatische Failoverprozess ist jedoch langsamer, da eine neue Maschine u. U. eine Weile


© 1999-2017 Citrix Systems, Inc. All rights reserved.

braucht, bis sie gestartet wird, und dadurch auch die Datenbank. Möglicherweise wird also der Dienst für Benutzer unterbrochen.

**Hinweis:** Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist. Weitere Informationen finden Sie im Artikel *Verbindungsleasing*.

Für den Fall, dass alle Controller einer Site ausfallen, können Sie den Virtual Delivery Agent so konfigurieren, dass er im Hochverfügbarkeitsmodus arbeitet, damit Benutzer weiterhin auf Desktops und Anwendungen zugreifen und diese verwenden können. Im Hochverfügbarkeitsmodus akzeptiert der VDA direkte ICA-Verbindungen von Benutzern anstelle von durch den Controller vermittelten Verbindungen. Dieses Feature ist nur zur Verwendung in dem seltenen Fall, dass die Kommunikation mit allen Controllern fehlschlägt, vorgesehen. Es ist keine Alternative zu anderen Hochverfügbarkeitslösungen. Weitere Informationen finden Sie unter CTX127564.

# Installieren der Datenbanksoftware

Standardmäßig wird zusammen mit dem ersten Delivery Controller SQL Server Express installiert, wenn keine andere Instanz von SQL Server auf dem Server erkannt wird. Dies genügt normalerweise für Machbarkeitsstudien oder Testumgebungen. SQL Server Express unterstützt jedoch keine Microsoft-Features für hohe Verfügbarkeit.

Diese Installation verwendet die Standarddienstkonten und -privilegien von Windows. Informationen zu diesen Standards und dem Hinzufügen von Windows-Dienstkonten zur sysadmin-Rolle finden Sie in der Microsoft-Dokumentation. In dieser Konfiguration verwendet der Controller das Netzwerkdienstkonto. Der Controller erfordert keine weiteren SQL Server-Rollen oder -Berechtigungen.

Bei Bedarf können Sie zum Ausblenden der Datenbankinstanz die Option **Instanz ausblenden** wählen. Geben Sie beim Konfigurieren der Datenbankadresse in Studio die statische Portnummer statt des Namens ein. Informationen zum Ausblenden einer Instanz des SQL Server-Datenbankmoduls finden Sie in der Dokumentation von Microsoft.

In den meisten Produktionsbereitstellungen und in Bereitstellungen, in denen Microsoft-Features für hohe Verfügbarkeit verwendet werden, muss eine andere (unterstützte) SQL Server-Version als SQL Server Express auf den anderen Computern (als dem mit dem ersten Controller) installiert werden. In dem Artikel über die Systemanforderungen werden die unterstützten SQL Server-Versionen aufgeführt. Die Datenbanken können auf einem oder mehreren Computern residieren.

Stellen Sie sicher, dass die SQL Server-Software installiert ist, bevor Sie eine Site erstellen. Sie müssen keine Datenbank erstellen, wenn Sie es jedoch tun, muss sie leer sein. Außerdem empfiehlt sich das Konfigurieren von Microsoft-Features für hohe Verfügbarkeit.

Halten Sie die SQL Server-Installation mit Windows Update auf dem neuesten Stand.

# Einrichten der Datenbanken mit dem Assistenten für die Siteerstellung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Legen Sie Namen und Speicherorte der Datenbanken auf der Seite **Datenbanken** des Assistenten für die Siteerstellung fest (s. *Datenbankadressformate* weiter unten). Zur Vermeidung von Fehlern bei künftigen Abfragen von Monitor Service durch Director verwenden Sie keine Leerzeichen im Namen der Überwachungsdatenbank.

Die Seite **Datenbanken** bietet zwei Optionen zum Einrichten der Datenbanken: automatisch und Skriptverwendung. Normalerweise können Sie die automatische Erstellung wählen, wenn Sie die erforderlichen Berechtigungen für die Datenbank haben (Studio-Benutzer und Citrix Administrator). Weitere Informationen finden Sie unter "Für die Einrichtung von Datenbanken erforderliche Berechtigungen" weiter unten.

Sie können den Speicherort einer Datenbank nach Erstellen der Site ändern. Weitere Informationen finden Sie unter "Ändern des Datenbankspeicherorts" weiter unten.

Zum Konfigurieren einer Site für die Verwendung einer gespiegelten Datenbank führen Sie die folgenden Verfahren durch und fahren Sie dann mit der automatischen oder skriptbasierten Einrichtung fort:

1. Installieren Sie SQL Server auf zwei Servern, A und B.
2. Erstellen Sie auf Server A die Datenbank, die als Hauptdatenbank verwendet werden soll. Sichern Sie die Datenbank auf Server A und kopieren Sie sie anschließend auf Server B.
3. Stellen Sie auf Server B die Sicherungsdatei wieder her.
4. Starten Sie die Spiegelung auf Server A.

**Tipp:** Um die Spiegelung nach dem Erstellen der Site zu überprüfen, führen Sie das PowerShell-Cmdlet **get-configdbconnection** aus, um sicherzustellen, dass der Failoverpartner in der Verbindungszeichenfolge für die Spiegelung eingerichtet wurde.

Wenn Sie später einen Delivery Controller in einer gespiegelten Datenbankumgebung hinzufügen, verschieben oder entfernen möchten, gehen Sie wie unter "Delivery Controller" beschrieben vor.

### Automatische Einrichtung

Wenn Sie die erforderlichen Datenbankberechtigungen haben, wählen Sie auf der Seite **Datenbanken** des Assistenten für die Siteerstellung die Option "Datenbanken mit Studio erstellen und einrichten" und geben Sie die Namen und Adressen der Hauptdatenbanken ein.

Gibt es an einer von Ihnen angegebenen Adresse eine Datenbank, muss sie leer sein. Gibt es an der angegebenen Adresse keine Datenbank, wird eine entsprechende Meldung angezeigt und Sie werden gefragt, ob eine Datenbank erstellt werden soll. Wenn Sie dies bejahen, werden die Datenbanken erstellt und die Initialisierungsskripts für die Haupt- und Replikatdatenbanken ausgeführt.

### Einrichtung per Skript

Wenn Sie nicht die erforderlichen Datenbankberechtigungen haben, muss eine andere Person mit diesen Berechtigungen, z. B. ein Datenbankadministrator, helfen. Verfahren:

1. Wählen Sie im Assistenten für die Siteerstellung die Option **Skripts generieren**. Es werden insgesamt sechs Skripts für die drei Datenbanken erstellt, eines für jede Hauptdatenbank und eines für jedes Replikat. Sie können den Speicherort für die Skripts festlegen.
2. Geben Sie die Skripts Ihrem Datenbankadministrator. Der Assistent für die Siteerstellung hält an diesem Punkt automatisch an und wenn Sie später zurückkehren, werden Sie aufgefordert, die Siteerstellung fortzusetzen.

Der Datenbankadministrator erstellt dann die Datenbanken. Die Datenbanken müssen folgende Merkmale aufweisen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Sortierung, die in "_CI_AS_KS" endet. Citrix empfiehlt die Verwendung einer Sortierung, die in "_100_CI_AS_KS" endet.
- Zur Gewährleistung der optimalen Leistung aktivieren Sie den SQL Server-Read-Committed-Snapshot. Weitere Informationen finden Sie unter CTX 137161.
- Features für hohe Verfügbarkeit sollten nach Bedarf konfiguriert werden.
- Zum Konfigurieren der Spiegelung legen Sie für die Datenbank das vollständige Wiederherstellungsmodell fest (Standardeinstellung ist das einfache Wiederherstellungsmodell). Sichern Sie die Hauptdatenbank und kopieren Sie die Sicherungsdatei auf den Spiegelserver. Stellen Sie in der Spiegeldatenbank die Sicherungsdatei auf dem Spiegelserver wieder her. Starten Sie dann die Spiegelung auf dem Hauptserver.

Der Datenbankadministrator führt jedes xxx_Replica.sql-Skript mit dem SQLCMD-Befehlszeilenprogramm oder mit SQL Server Management Studio im SQLCMD-Modus in den SQL Server-Datenbankinstanzen mit hoher Verfügbarkeit (sofern konfiguriert) aus und dann jedes xxx_Principal.sql-Skript in den Hauptinstanzen der SQL Server-Datenbank. Weitere Informationen zu SQLCMD können Sie der Dokumentation von Microsoft entnehmen.

Wenn alle Skripts erfolgreich ausgeführt wurden, übergibt der Datenbankadministrator dem Citrix Administrator die drei Hauptdatenbankadressen.

In Studio werden Sie aufgefordert, die Siteerstellung fortzusetzen, und die Seite **Datenbanken** wird wieder angezeigt. Geben Sie die Adressen ein. Wenn einer der Server mit einer Datenbank nicht erreicht werden kann, wird eine Fehlermeldung angezeigt.

# Für die Einrichtung von Datenbanken erforderliche Berechtigungen

Zum Erstellen und Initialisieren der Datenbanken (bzw. zum Ändern des Speicherorts einer Datenbank) müssen Sie lokaler Administrator und Domänenbenutzer sein. Sie benötigen zudem bestimmte SQL Server-Berechtigungen. Die nachfolgend aufgeführten Berechtigungen können über eine Active Directory-Gruppenmitgliedschaft explizit konfiguriert oder erworben werden. Wenn Ihre Studio-Anmeldeinformationen diese Berechtigungen nicht umfassen, werden Sie aufgefordert, Benutzeranmeldeinformationen für SQL Server einzugeben.

| Vorgang | Zweck | Serverrolle | Datenbankrolle |
|---|---|---|---|
| Erstellen einer Datenbank | Erstellen einer geeigneten leeren Datenbank | dbcreator | |
| Erstellen eines Schemas | Erstellen aller dienstspezifischen Schemas und Hinzufügen des ersten Controllers zur Site | securityadmin * | db_owner |
| Hinzufügen eines Controllers | Hinzufügen eines weiteren Controllers (zusätzlich zum ersten) zur Site | securityadmin * | db_owner |
| Hinzufügen eines Controllers | Hinzufügen einer Controller-Anmeldung zu dem Datenbankserver, der derzeit die | securityadmin * | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | | | |
|---|---|---|---|
| (Spiegelungsserver) | Spiegelrolle einer gespiegelten Datenbank hat | | |
| Aktualisieren eines Schemas | Anwenden von Aktualisierungen oder Hotfixes auf das Schema | | db_owner |

* Zwar ist die securityadmin-Serverrolle technisch restriktiver als die sysadmin-Serverrolle, aber in der Praxis ist sie als gleichwertig anzusehen.

Wenn Sie diese Vorgänge mit Studio ausführen, muss das Benutzerkonto Mitglied der sysadmin-Serverrolle sein.

# Datenbankadressformate

Datenbankadressen können in einem der folgenden Formate angegeben werden:

- Servername
- Servername\Instanzname
- Servername,Portnummer

Geben Sie für AlwaysOn-Verfügbarkeitsgruppen den Listener der Gruppe im Feld "Speicherort" an.

# Ändern des Speicherorts von Datenbanken

Nachdem Sie eine Site erstellt haben, können Sie den Speicherort der Datenbanken ändern. Berücksichtigen Sie Folgendes, wenn Sie den Speicherort einer Datenbank ändern:

- Die Daten werden nicht aus der bestehenden Datenbank in die neue Datenbank importiert.
- Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden.
- Der erste Protokolleintrag in der neuen Datenbank gibt an, dass eine Datenbankänderung stattfand, die vorherige Datenbank wird jedoch nicht angegeben.

Sie können den Speicherort der Konfigurationsprotokollierungsdatenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist.

Ändern des Datenbankspeicherorts

1. Vergewissern Sie sich, dass eine unterstützte Version von Microsoft SQL Server auf dem Server installiert ist, auf dem die Datenbank residieren soll. Richten Sie Features für hohe Verfügbarkeit nach Bedarf ein.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration** aus.
3. Wählen Sie die Datenbank aus, für die Sie einen neuen Speicherort angeben möchten, und wählen Sie dann im Aktionsbereich **Datenbank ändern** aus.
4. Geben Sie den neuen Speicherort und den Datenbanknamen ein.
5. Wenn die Datenbank von Studio erstellt werden soll und Sie die notwendigen Berechtigungen haben, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**. Die Datenbank wird dann automatisch erstellt. Studio versucht, mit Ihren Anmeldeinformationen auf die Datenbank zuzugreifen; wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Datenbank hochgeladen. Die Anmeldeinformationen werden nur für den Zeitraum der Datenbankerstellung gespeichert.

6. Wenn die Datenbank nicht von Studio erstellt werden soll oder Sie die erforderliche Berechtigung nicht haben, klicken Sie auf **Skript generieren**. Die generierten Skripts enthalten Anweisungen, wie Sie die Datenbank und ggf. die Spiegeldatenbank manuell erstellen. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bereitstellungsmethoden

Jul 08, 2016

Es ist eine Herausforderung, die Anforderungen aller Benutzer mit einer Virtualisierungsbereitstellung erfüllen. Mit XenApp und XenDesktop können Administratoren die Benutzererfahrungen mit verschiedenen Methoden, die auch als FlexCast-Modelle bezeichnet werden, anpassen.

Diese Bereitstellungsmethoden, von denen jede ihre Vor- und Nachteile hat, bieten die beste Benutzererfahrung für jeden Anwendungsfall.

## Mobilisieren von Windows-Anwendungen auf Mobilgeräten

Touchscreen-Geräte, wie Tablets und Smartphones, sind jetzt Standard in Mobilität. Wenn Windows-basierte Anwendungen auf ihnen ausgeführt werden, die normalerweise auf großen Bildschirmen angezeigt werden und für volle Funktionalität Klicken mit der rechten Maustaste erfordern, können diese Geräte Probleme verursachen.

XenApp mit Citrix Receiver bietet eine sichere Lösung, sodass die Benutzer von Mobilgeräten Zugriff auf alle Funktionen ihrer Windows-basierten Apps haben, ohne dass diese kostenaufwendig für native mobile Plattformen umgeschrieben werden müssen.

Die Bereitstellungsmethode der mit XenApp veröffentlichten Anwendungen verwendet die HDX-Mobiltechnologie, die die mit der Mobilisierung von Windows-Anwendungen assoziierten Probleme löst. Mit dieser Methode können Windows-Anwendungen für die Toucheingabe umgestaltet werden, während Features wie Mehrfingerbewegungen, native Menüsteuerung, Kamera und GPS-Funktionen erhalten bleiben. Viele Touchfeatures sind nativ in XenApp und XenDesktop und zu ihrer Aktivierung sind keine Änderungen am Anwendungsquellcode nötig.

Zu diesen Features gehören Folgende:

- Automatische Anzeige der Tastatur, wenn ein bearbeitbares Feld den Fokus erhält
- Größeres Auswahlsteuerelement ersetzt Windows-Kombinationsfeld-Steuerelement
- Mehrfingergesten, z. B. Vergrößern und Verkleinern mit zwei Fingern
- Trägheitssensitiver Bildlauf
- Touchpad oder direkte Cursornavigation

## Verringern der Aktualisierungskosten für PCs

Das Aktualisieren von physischen Maschinen ist eine große Aufgabe, der sich viele Unternehmen alle drei bis fünf Jahre stellen müssen, besonders, wenn ein Unternehmen bei Betriebssystemen und Anwendungen immer auf dem neuesten Stand sein muss. Wachsende Unternehmen sehen sich zudem hohen Kosten für das Hinzufügen von neuen Maschinen zum Netzwerk gegenüber.

Mit der Bereitstellungsmethode eines VDI mit Personal vDisk können Einzelbenutzern vollständig personalisierte Desktopbetriebssysteme auf jeder Maschine oder jedem Thin Client mit Serverressourcen bereitgestellt werden. Administratoren können virtuelle Maschinen erstellen, deren Ressourcen, z. B. Verarbeitung, Arbeitsspeicher und Speicher, sich im Datencenter des Netzwerks befinden.

Dadurch kann das Leben älterer Maschinen verlängert werden, Software ist auf dem aktuellen Stand und Ausfallzeiten bei Upgrades werden minimiert.

## Sicheren Zugriff auf virtuelle Apps und Desktops für Vertragsunternehmen und Partner sicherstellen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Netzwerksicherheit ist ein wachsendes Problem, besonders bei der Arbeit mit Vertragsunternehmen, Partnern und gelegentlichen Mitarbeitern von Fremdfirmen, die Zugriff auf Unternehmensapps und Daten benötigen. Die Mitarbeiter benötigen möglicherweise auch leihweise Laptops oder andere Geräte, die zusätzliche Kosten verursachen.

Daten, Anwendungen und Desktops sind bei XenDesktop und XenApp hinter der Firewall des sicheren Netzwerks gespeichert, sodass Endbenutzer nur die Ein - und Ausgabevorgänge der Benutzergeräte wie Tastatureingaben, Mausklicks, Audio und Bildschirmaktualisierungen übermitteln. Durch die Verwaltung dieser Ressourcen in einem Datencenter bieten XenDesktop und XenApp eine sicherere Remotezugriffslösung als das übliche SSL VPN.

Bei einer VDI-Bereitstellung mit Personal vDisk können Administratoren Thin Clients oder die persönlichen Geräte von Benutzern nutzen, indem sie eine virtuelle Maschine auf einem Netzwerkserver erstellen und ein Betriebssystem für einzelne Benutzer anbieten. Auf diese Weise können IT-Abteilungen die Sicherheit gegenüber Mitarbeitern von Vertragsunternehmen aufrechterhalten, ohne zusätzliches teures Gerät kaufen zu müssen.

### Beschleunigte Migration

Beim Wechsel zu einem neuen Betriebssystem kann es eine Herausforderung sein, Legacy- und nicht kompatiblen Anwendungen bereitzustellen.

Mit VM-gehosteten Apps können Benutzer ältere Anwendungen über Citrix Receiver auf der aktualisierten virtuellen Maschine ohne Kompatibilitätsprobleme ausführen. Dadurch haben IT-Mitarbeiter mehr Zeit, Kompatibilitätsprobleme zu testen und zu beheben, Benutzern den Übergang zu erleichtern und die Effizienz bei Helpdeskanrufen zu erhöhen.

Zusätzliche Vorteile bei der Verwendung von XenDesktop während der Migration sind u. a.:

- Reduzierte Komplexität von Desktops
- Verbesserte Steuerung für IT-Mitarbeiter
- Erhöhte Flexibilität der Endbenutzer im Hinblick auf Geräte und Arbeitsplatz

### Virtualisierung professioneller 3-D-Grafikanwendungen für Designer und Techniker

Viele Designunternehmen und Herstellerfirmen sind stark auf professionelle 3-D-Grafikanwendungen angewiesen. Die Kosten der für diese Art Software erforderlichen leistungsfähigen Hardware sind für diese Unternehmen eine große finanzielle Belastung. Dazu kommen logistische Probleme durch die Freigabe großer Designdateien über FTP, E-Mail und andere Ad-hoc-Methoden.

Bei der XenDesktop-Bereitstellungsmethode für gehostete physische Desktops wird ein Desktopimage auf Arbeitsstationen und Bladeservern bereitgestellt, ohne dass Hypervisors benötigt werden, um grafikintensive 3-D-Anwendungen auf einem systemeigenen Betriebssystem auszuführen.

Alle Dateien werden in einem zentralen Datencenter im Netzwerk gespeichert und große Designdateien können schneller und sicherer für andere Benutzer im Netzwerk freigegeben werden, da die Dateien nicht zwischen Arbeitsstationen übertragen werden müssen.

### Transformation von Callcentern

Unternehmen mit großen Callcentern stehen vor der Herausforderung, zu Spitzenzeiten genügend Maschinen und zu anderen Zeiten nicht zu viele Maschinen im Einsatz zu haben.

Die gepoolte VDI-Bereitstellungsmethode bietet dynamischen Zugriff auf einen standardisierten Desktop für viele Benutzer zu minimalen Kosten. Die gepoolten Maschinen werden pro Sitzung nach dem Windhundprinzip zugeteilt.

Bei diesen virtuellen Maschinen fällt weniger alltägliche Verwaltung an, da während der Sitzung vorgenommene Änderungen

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

verworfen werden, wenn der Benutzer sich abmeldet. Dies erhöht auch die Sicherheit.

Von XenApp gehostete Desktops ist eine weitere Bereitstellungsmethode, die sich für Callcenter eignet. Bei dieser Methode werden mehrere Benutzerdesktops auf einem serverbasierten Betriebssystem gehostet.

Dies ist eine kosteneffizientere Methode als die gepoolte VDI-Bereitstellung, aber bei von XenApp gehosteten Desktops haben Benutzer keine Berechtigungen, um Anwendungen zu installieren, Systemeinstellungen zu ändern oder den Server neu zu starten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Mit XenApp veröffentlichte Anwendungen und Desktops

Jul 08, 2016

Verwenden Sie Serverbetriebssystemmaschinen zum Bereitstellen von mit XenApp veröffentlichten Anwendungen und Desktops.

**Anwendungsfall**

- Gewünscht wird eine kostengünstige, serverbasierte Bereitstellung, um die Kosten für die Bereitstellung von Anwendungen für eine große Anzahl von Benutzern gering zu halten, und gleichzeitig eine sichere High-Definition-Benutzererfahrung zu bieten.
- Die Benutzer führen vordefinierte Aufgaben aus, es wird keine Personalisierung oder kein Offlinezugriff auf Anwendungen benötigt. Hierzu können aufgabenorientierte Mitarbeiter, wie z. B. Callcenter- und Einzelhandelsarbeitskräfte gehören, oder Benutzer, die Arbeitsstationen gemeinsam verwenden.
- Anwendungstypen: beliebig

**Vorteile und Überlegungen**

- Verwaltbare und skalierbare Lösung für das Datenzentrum.
- Kosteneffektivste Lösung für die Anwendungsbereitstellung.
- Gehostete Anwendungen werden zentral verwaltet und Benutzer können die Anwendung nicht ändern, wodurch eine konsistente, sichere und zuverlässige Benutzererfahrung bereitgestellt wird.
- Benutzer müssen online sein, um auf ihre Anwendungen zuzugreifen.

**Benutzererfahrung**

- Benutzer fordern eine oder mehrere Anwendungen von StoreFront über ihr Startmenü oder eine von Ihnen vorgegebene URL an.
- Anwendungen werden virtuell bereitgestellt und in High Definition auf Benutzergeräten angezeigt.
- Abhängig von den Profileinstellungen werden Benutzeränderungen gespeichert, wenn die Anwendungssitzung des Benutzers beendet wird. Andernfalls werden die Änderungen werden gelöscht.

**Verarbeiten, Hosten und Bereitstellen von Anwendungen**

- Die Anwendungsverarbeitung findet auf den Hostingmaschinen statt, nicht auf den Benutzergeräten. Die Hostingmaschine kann eine physische oder eine virtuelle Maschine sein.
- Anwendungen und Desktops sind auf einer Serverbetriebssystemmaschine gespeichert.
- Maschinen werden über Maschinenkataloge verfügbar gemacht.
- Maschinen aus Maschinenkatalogen sind in Bereitstellungsgruppen organisiert, die Benutzergruppen dieselben Anwendungen bereitstellen.
- Serverbetriebssystemmaschinen unterstützen Bereitstellungsgruppen, die Desktops oder Anwendungen oder beides hosten.

**Sitzungsverwaltung und -zuweisung**

- Auf Serverbetriebssystemmaschinen werden mehrere Sitzungen auf einer einzelnen Maschinen ausgeführt, über die mehrere Anwendungen und Desktops an mehrere, gleichzeitig verbundene Benutzer bereitgestellt werden. Jeder


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Benutzer benötigt eine einzelne Sitzung, um die gehosteten Anwendungen auszuführen.

Beispiel: Ein Benutzer meldet sich an und fordert eine Anwendung an. Eine der Sitzungen auf dieser Maschine ist für die anderen Benutzer nicht mehr verfügbar. Ein zweiter Benutzer meldet sich an und fordert eine Anwendung an, die von dieser Maschine gehostet wird. Eine zweite Sitzung auf derselben Maschine ist damit jetzt nicht verfügbar. Wenn beide Benutzer weitere Anwendungen anfordern, werden keine zusätzlichen Sitzungen benötigt, da ein Benutzer mehrere Anwendungen in der gleichen Sitzung ausführen kann. Wenn zwei weitere Benutzer sich anmelden und Desktops anfordern, und zwei Sitzungen auf derselben Maschine verfügbar sind, hostet diese eine Maschine nun vier Sitzungen für vier verschiedene Benutzer.

- In der Bereitstellungsgruppe, der ein Benutzer zugewiesen ist, wird eine Maschine auf einem Server mit der geringsten Last ausgewählt. Ein Computer mit Sitzungsverfügbarkeit wird nach dem Zufallsprinzip zugewiesen und stellt einem Benutzer bei der Anmeldung Anwendungen bereit.

Bereitstellen mit XenApp veröffentlichter Anwendungen und Desktops

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Serverbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen von Desktops und Anwendungen. Wenn Sie Anwendungen bereitstellen, wählen Sie die gewünschten aus.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# VM-gehostete Apps

Jul 08, 2016

Bereitstellen VM-gehosteter Anwendungen über Desktopbetriebssystemmaschinen

**Anwendungsfall**

- Gewünscht wird eine clientbasierte Anwendungsbereitstellungslösung, die eine sichere, zentrale Verwaltung bietet und eine große Anzahl von Benutzern pro Hostserver (oder Hypervisor) unterstützt und Benutzern Anwendungen bereitstellt, die problemlos in High Definition angezeigt werden.
- Benutzer sind interne und externe Auftragnehmer, Partner aus Fremdunternehmen und andere vorläufige Teammitglieder. Sie benötigen keinen Offlinezugriff auf gehostete Anwendungen.
- Anwendungsarten: Anwendungen, die möglicherweise nicht gut mit anderen Anwendungen funktionieren oder mit dem Betriebssystem interagieren, z. B. .NET Framework. Dieser Typ von Anwendungen eignet sich gut für das Hosting auf virtuellen Maschinen.

  Anwendungen, die auf älteren Betriebssystemen (z. B. Windows XP oder Windows Vista) und älteren Architekturen (z. B. 32 Bit oder 16 Bit) ausgeführt werden. Durch Isolieren jeder Anwendung auf einer eigenen virtuellen Maschine werden die anderen Benutzer bei Ausfall einer Maschine nicht beeinträchtigt.

**Vorteile und Überlegungen**

- Anwendungen und Desktops auf dem Masterimage werden sicher verwaltet, gehostet und auf Maschinen im Datenzentrum ausgeführt, womit eine kosteneffektivere Lösung für die Anwendungsbereitstellung bereitgestellt wird.
- Die Benutzer können bei der Anmeldung willkürlich einer Maschine in einer Bereitstellungsgruppe zugewiesen werden, die für das Hosting einer Anwendung konfiguriert ist. Sie können auch einem einzelnen Benutzer eine einzelne Maschine für die Anwendungsbereitstellung jedes Mal statisch zuweisen, wenn sich der Benutzer anmeldet. Bei statisch zugewiesenen Maschinen kann der Benutzer eigene Anwendungen auf der virtuellen Maschine installieren und verwalten.
- Das Ausführen mehrerer Sitzungen auf Desktopbetriebssystemmaschinen wird nicht unterstützt. Daher beansprucht jeder Benutzer bei der Anmeldung eine einzelne Maschine innerhalb einer Bereitstellungsgruppe und der Zugriff auf die Anwendungen muss online erfolgen.
- Bei dieser Methode werden die Serverressourcen für die Verarbeitung von Anwendungen sowie der Speicher für die persönlichen vDisks der Benutzer erhöht.

**Benutzererfahrung**

Die gleiche nahtlose Anwendungserfahrung wie mit gehosteten, freigegebenen Anwendungen auf Serverbetriebssystemmaschinen.

**Verarbeiten, Hosten und Bereitstellen von Anwendungen**

Wie bei Serverbetriebssystemmaschinen, nur dass es sich um virtuelle Desktopbetriebssystemmaschinen handelt.

**Sitzungsverwaltung und -zuweisung**

- Desktopbetriebssystemmaschinen führen eine Desktopsitzung von einer Maschine aus. Nur beim Zugriff auf Anwendungen: Ein Benutzer kann mehrere Anwendungen verwenden (und ist nicht auf eine Anwendung eingeschränkt), da das Betriebssystem jede Anwendung als eine neue Sitzung ansieht.
- Innerhalb einer Bereitstellungsgruppe erhalten Benutzer bei der Anmeldung entweder statischen Zugriff auf eine


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Maschine (d. h. bei jeder Anmeldung die gleiche Maschine) oder es wird ihnen eine Maschine nach Sitzungsverfügbarkeit zugewiesen.

Bereitstellen von VM-gehosteten Apps:

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Desktopbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Entscheiden Sie beim Definieren der Desktopdarstellung für den Maschinenkatalog, ob Benutzer bei jeder Anmeldung mit einer neuen VM oder mit derselben VM verbunden werden.
4. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen der Anwendungen für Benutzer.
5. Wählen Sie in der Liste der installierten Anwendungen die Anwendung aus, die Sie bereitstellen möchten.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# VDI-Desktops

Jul 08, 2016

Verwenden Sie Desktopbetriebssystemmaschinen zum Bereitstellen von VDI-Desktops.

VDI-Desktops werden auf virtuellen Maschinen gehostet und bieten jedem Benutzer ein Desktopbetriebssystem.

VDI-Desktops benötigen mehr Ressourcen als mit XenApp veröffentlichte Desktops, aber es ist nicht erforderlich, dass die auf ihnen installierten Anwendungen serverbasierte Betriebssysteme unterstützen. Abhängig vom ausgewählten Typ des VDI-Desktops kann der Desktop einzelnen Benutzern zugewiesen werden und von den Benutzern in hohem Maße personalisiert werden.

Beim Erstellen eines Maschinenkatalogs für VDI-Desktops erstellen Sie einen der folgenden Desktoptypen:

- Zufällige, nicht beständige Desktops (gepoolte VDI-Desktops): Jedes Mal, wenn Benutzer sich anmelden, um einen dieser Desktops zu verwenden, wird eine Verbindung zu einem dynamisch ausgewählten Desktop in einem Pool von Desktops erstellt, die alle auf einem Masterimage basieren. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- Statischer, nicht beständiger Desktop: Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen dieser Desktops zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die alle auf einem Masterimage basieren. Daraufhin wird dem Benutzer jedes Mal, wenn er sich anmeldet, um einen der Desktops zu verwenden, derselbe Desktop wie beim ersten Mal zugewiesen. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- Statisch und permanent (VDI-Desktop mit persönlicher vDisk): Im Gegensatz zu anderen Typen der VDI-Desktops können diese Desktops vollständig personalisiert werden. Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen dieser Desktops zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die alle auf einem Masterimage basieren. Daraufhin wird dem Benutzer jedes Mal, wenn er sich anmeldet, um einen der Desktops zu verwenden, derselbe Desktop wie beim ersten Mal zugewiesen. Änderungen am Desktop bleiben beim Neustart der Maschine erhalten, da sie auf einer persönlichen vDisk gespeichert werden.

Bereitstellen von VDI-Desktops:

1. Erstellen Sie ein Masterimage mit einem unterstützten Windows-Desktopbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage. Entscheiden Sie beim Definieren der Desktopdarstellung für den Maschinenkatalog, ob Benutzer bei jeder Anmeldung mit einer neuen VM oder mit derselben VM verbunden werden, und legen Sie fest, ob Änderungen am Desktop beibehalten werden.
3. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen der Desktops für Benutzer.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installation und Konfiguration

Jul 15, 2016

Lesen Sie vor jedem Bereitstellungsschritt die Artikel, auf die verwiesen wird, um sich alle für die Bereitstellung erforderlichen Kenntnisse anzueignen.

Befolgen Sie bei der Bereitstellung von XenApp bzw. XenDesktop nachfolgend aufgeführte Reihenfolge.

# Vorbereiten

Lesen Sie den Artikel Vorbereiten der Installation und erledigen Sie alle erforderlichen Aufgaben. Dies umfasst:

- Kennenlernen von XenApp und XenDesktop – der Artikel enthält Quellen mit Informationen über Konzepte, Features, Unterschiede zu früheren Releases, Systemanforderungen und Datenbanken.
- Einrichten der Infrastruktur für Virtualisierung, Hosting und oder Support (falls verwendet)
- Einrichten der Maschinen, auf denen die Komponenten installiert werden
- Einrichten der Active Directory-Umgebung

Der Artikel enthält zudem Angaben zu den Informationen, die Sie bei der Installation der Komponenten und beim Aktivieren von Features auswählen oder angeben müssen.

Wenn Sie Linux-VDAs installieren möchten, lesen Sie vor der Installation die Artikel Installieren von VDAs unter Red Hat Linux und Installieren von VDAs unter SUSE Linux.

# Installieren der Kernkomponenten

Installieren Sie Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver und Citrix StoreFront. Sie können eine assistentengestützte grafische Oberfläche oder eine Befehlszeilenoberfläche für die skriptbasierte Installation verwenden. Bei beiden Methoden werden die meisten Voraussetzungen automatisch installiert.

# Erstellen einer Site

Wenn Sie nach der Installation der Kernkomponenten Studio starten, führt Sie der Assistent für die Siteerstellung automatisch durch die Erstellung einer Site.

# Installieren eines oder mehrerer Virtual Delivery Agents (VDAs)

Installieren Sie einen VDA auf einem Windows-Computer, entweder auf dem künftig zur Erstellung virtueller Maschinen genutzten Masterimage oder direkt auf jeder Maschine. Sie können eine grafische Benutzeroberfläche oder eine Befehlszeilenoberfläche verwenden. Beispielskripts werden bereitgestellt, wenn Sie die VDAs über Active Directory installieren möchten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bei Maschinen mit einem Linux-Betriebssystem befolgen Sie die Anweisungen für die Installation eines VDA unter Red Hat Linux bzw. unter SUSE Linux.

Für eine Remote-PC-Zugriff-Bereitstellung installieren Sie einen VDA für Desktopbetriebssysteme auf jedem Büro-PC. Verwenden Sie aus Effizienzzwecken die Befehlszeilenoberfläche des eigenständigen VDA-Installers und Ihre gewohnten Methoden zur elektronischen Softwareverteilung.

# Installieren optionaler Komponenten

Wenn Sie den universellen Druckserver von Citrix verwenden möchten, installieren Sie dessen Serverkomponente auf Ihren Druckservern. Sie können eine grafische Benutzeroberfläche oder eine Befehlszeilenoberfläche verwenden. Weitere Informationen finden Sie unter Bereitstellen von Druckern.

Damit StoreFront Authentifizierungsoptionen wie SAML-Assertions verwenden kann, installieren Sie den Citrix Federated Authentication Service und zwar möglichst auf einem Server, der keine anderen Citrix Komponenten enthält.

Sie können auch zusätzlichen Citrix Komponenten in die XenApp- oder XenDesktop-Bereitstellung integrieren. Beispiel:

- Provisioning Services ist eine optionale Komponente von XenApp und XenDesktop, mit der Maschinen durch das Streaming eines Masterimages auf die Zielgeräte bereitgestellt werden. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
- Citrix NetScaler Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren durch Richtlinien auf Anwendungsebene und durch Aktionssteuerung ermöglicht, den Zugriff auf Anwendungen und Daten zu sichern. Weitere Informationen finden Sie in der Dokumentation zu Citrix NetScaler Gateway.
- Citrix CloudBridge bietet eine Reihe von Geräten, die die WAN-Leistung optimieren. Weitere Informationen finden Sie in der Dokumentation zu Citrix CloudBridge.

Installationsanweisungen finden Sie in der Dokumentation für die jeweiligen Komponenten.

# Erstellen von Maschinenkatalogen

Nachdem Sie eine Site in Studio erstellt haben, werden Sie durch die Erstellung eines Maschinenkatalogs geführt.

Ein Katalog kann physische oder virtuelle Maschinen (VMs) enthalten. Virtuelle Maschinen können aus einem Masterimage erstellt werden. Wenn Sie einen unterstützten Hypervisor oder Clouddienst zum Bereitstellen von VMs verwenden möchten, müssen Sie zuerst ein Masterimage auf dem betreffenden Host erstellen. Bei der Erstellung des Katalogs geben Sie dann das Image an, das zum Erstellen von VMs verwendet werden soll.

# Erstellen einer Bereitstellungsgruppe

Nachdem Sie den ersten Maschinenkatalog in Studio erstellt haben, werden Sie durch die Erstellung einer Bereitstellungsgruppe geführt.

Bereitstellungsgruppen steuern, welche Benutzer auf Maschinen in einem Maschinenkatalog zugreifen können und welche Anwendungen ihnen zur Verfügung stehen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen einer Anwendungsgruppe (optional)

Nachdem Sie eine Bereitstellungsgruppe erstellt haben, können Sie wahlweise eine Anwendungsgruppe erstellen. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Vorbereiten der Installation

Jul 15, 2016

Dieser Abschnitt enthält folgende Themen:

- Allgemeiner Installationsleitfaden
- Angaben bei der Installation der Hauptkomponenten
- Leitfaden zur VDA-Installation
- Angaben bei der VDA-Installation

# Allgemeiner Installationsleitfaden

- Wenn Sie Produkt und Komponenten nicht ausreichend kennen, lesen Sie die Artikel unter Technische Übersicht. Wenn Sie derzeit XenApp 6.x oder eine Vorgängerversion ausführen, können Sie im Artikel Konzepte und Komponenten nachlesen, worin die Unterschiede zur 7.x-Version von XenApp und XenDesktop bestehen.
- Bei der Planung der Bereitstellung konsultieren Sie die Artikel unter Sicherheit.
- Informieren Sie sich über bekannte Probleme, die bei der Installation auftreten können.
- Wenn Sie einen unterstützten Hypervisor oder Clouddienst für virtuelle Maschinen zur Bereitstellung von Anwendungen und Desktops verwenden, können Sie nach der Installation der Komponenten beim Erstellen einer Site die erste Verbindung mit diesem Host einrichten. Sie können die Virtualisierungsumgebung allerdings schon vorher konfigurieren. Konsultieren Sie dabei die hier aufgeführten Informationsquellen.
- Wenn Sie Microsoft System Center Configuration Manager zum Verwalten des Zugriffs auf Anwendungen und Desktops verwenden, lesen Sie diesen Artikel.
- Ist für eine Komponente .NET erforderlich, wird die erforderliche .NET Version vom Installationsprogramm bereitgestellt, wenn sie nicht vorhanden ist. Die .NET-Installation erfordert ggf. einen Neustart der Maschine.
- Der Artikel Datenbanken enthält Informationen über die Systemdatenbanken und deren Konfiguration. Während der Installation des Controllers können Sie wählen, ob Microsoft SQL Server 2012 Express auf demselben Server installiert werden soll. Das Gros der Datenbankinformationen konfigurieren Sie beim Erstellen einer Site, nachdem Sie die Kernkomponenten installiert haben.
- Wenn Sie den Citrix Lizenzserver installieren, wird das Benutzerkonto automatisch zum Volladministrator auf dem Lizenzserver. Weitere Informationen finden Sie im Artikel Delegierte Administration.
- Beim Erstellen von Objekten vor, während und nach der Installation müssen Sie eindeutige Namen für jedes Objekt (Netzwerke, Gruppen, Kataloge und Ressourcen) eingeben.
- Bei Installationsproblemen wird der Prozess angehalten und eine Fehlermeldung angezeigt. Komponenten, die erfolgreich installiert werden, bleiben gespeichert; sie müssen nicht neu installiert werden.
- Citrix Studio wird nach dem Abschluss der Installation automatisch gestartet. Bei Verwendung der grafischen Oberfläche können Sie diese Aktion auf der letzten Seite des Assistenten deaktivieren.
- Sie können die Kernkomponenten und Virtual Delivery Agents (VDAs) mit dem im Produkt-ISO-Image enthaltenen Installationsprogramm (dem "Produktinstallationsprogramm") installieren. Zum Installieren von VDAs können Sie neben dem Produktinstallationsprogramm auch das eigenständige VDA-Installationsprogramm verwenden. Letzteres kann von der Produkt-Downloadseite im Internet heruntergeladen werden. Beide Programme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.
- Das Produktinstallationsmedium enthält Beispielskripts, um VDAs für Gruppen von Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch auf einzelne Maschinen anwenden und sie zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services


© 1999-2017 Citrix Systems, Inc. All rights reserved.

verwendet werden. Weitere Informationen finden Sie im Artikel Installieren von VDAs mit Skripts.

- Die Serverkomponente (UpsServer) des universellen Druckserver können Sie mit der grafischen Oberfläche oder der Befehlszeilenschnittstelle des Produktinstallationsprogramms auf den Druckservern installieren. Die Produktdownloadseite im Internet enthält ggf. UpsServer-Pakete zum Herunterladen. Weitere Informationen finden Sie unter Bereitstellen von Druckern.
- Sie können den Verbundauthentifizierungsdienst mit dem Produktinstallationsprogramm installieren.
- Wenn Sie die Komponenten installieren, werden automatisch Analysedaten gesammelt. Wenn Sie mit der grafischen Oberfläche des Produktinstallationsprogramms einen Delivery Controller oder VDA installieren, können Sie angeben, ob Sie an Call Home teilnehmen möchten Weitere Informationen über die beiden Features finden Sie im Artikel zu Citrix Insight Services.
- Citrix Receiver für Mac und Citrix Receiver für Linux sind nicht mehr im Produkt-ISO-Image enthalten. Sie oder die Benutzer können diese Citrix Receiver-Versionen von der Citrix Website herunterladen und installieren. Alternativ können Sie diese Citrix Receiver-Versionen auf dem StoreFront-Server zur Verfügung stellen. Informationen hierzu finden Sie im Abschnitt Verfügbarmachen von Citrix Receiver-Installationsdateien auf dem Server in der Dokumentation zu StoreFront 3.0.x bzw. in der Dokumentation zu der von Ihnen verwendeten StoreFront-Version.

### Berechtigungen

Auf den Maschinen, auf denen Sie die Komponenten installieren, müssen Sie Domänenbenutzer und lokaler Administrator sein.

Für die Installation mit dem eigenständigen Installationsprogramm benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**.

Konfigurieren Sie die Active Directory-Domäne vor Beginn der Installation.

- Der Artikel Systemanforderungen enthält eine Liste der unterstützten Active Directory-Funktionsebenen. Der Artikel Active Directory enthält zusätzliche Informationen zu unterstützten Elementen.
- Sie müssen mindestens einen Domänencontroller mit Active Directory-Domänendiensten ausführen.
- Versuchen Sie nicht, Komponenten auf einem Domänencontroller zu installieren.
- Verwenden Sie keinen Schrägstrich (/), wenn Sie in Studio Namen für Organisationseinheiten festlegen.
- Weitere Informationen finden Sie in der Dokumentation von Microsoft zur Konfiguration von Active Directory.

### Installationsorte

Legen Sie fest, wo die Komponenten installiert werden, und bereiten Sie die Maschinen und Betriebssysteme vor.

- Der Artikel Systemanforderungen enthält Informationen über die unterstützten Betriebssysteme und Versionen für Controller, Studio, Citrix Director, Virtualisierungsressourcen (Hosts) und VDAs. Die meisten Komponentenvoraussetzungen werden automatisch installiert. Ausnahmen werden in dem Artikel aufgeführt. In den Dokumenten zu Citrix StoreFront und Citrix Lizenzserver finden Sie Angaben zu den unterstützten Plattformen.
- Sie können die Kernkomponenten auf dem gleichen Server oder auf unterschiedlichen Servern installieren. Um beispielsweise eine kleinere Bereitstellung remote zu verwalten, können Sie Studio auf einer anderen Maschine installieren als den Server, auf dem der Controller installiert wurde. Um zukünftige Erweiterungen zu ermöglichen, sollten Sie die Komponenten auf verschiedenen Servern installieren, z. B. den Lizenzserver und Director auf unterschiedlichen Servern.
- Sie können den Delivery Controller und den Virtual Delivery Agent für Windows-Serverbetriebssysteme auf demselben Server installieren. Starten Sie hierfür das Installationsprogramm und wählen Sie den Delivery Controller (sowie alle weiteren Kernkomponenten für diese Maschine). Starten Sie dann das Installationsprogramm erneut und wählen Sie den


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent für Windows-Serverbetriebssysteme.
- Installieren Sie keine Komponenten auf Domänencontrollern.
- Die Installation eines Controllers auf einem Knoten in einer SQL-Cluster- oder Spiegelungsinstallation oder auf einem Server mit Hyper-V wird nicht unterstützt.
- Installieren Sie Studio nicht auf einem Server, auf dem XenApp 6.5 Feature Pack 2 für Windows Server 2008 R2 oder eine frühere Version von XenApp ausgeführt wird.
- Stellen Sie sicher, dass für jedes Betriebssystem die neuesten Updates ausgeführt wurden.
- Stellen Sie sicher, dass bei allen Maschinen die Systemuhren synchronisiert sind. Die Synchronisierung wird für die Kerberos-Infrastruktur benötigt, die die Kommunikation zwischen den Maschinen sichert.

# Angaben bei der Installation der Hauptkomponenten

In den folgenden Abschnitten werden die Parameter erläutert, die Sie bei der Installation festlegen. Die Beschreibung folgt den Schritten des Assistenten der grafischen Oberfläche; entsprechende Optionen für die Befehlszeilenschnittstelle werden ebenfalls aufgeführt. In den Artikeln zur Installation wird erläutert, wie Sie den Assistenten starten und Befehle mit Optionen eingeben.

Komponenten werden standardmäßig unter C:\Programme\Citrix installiert. Sie können auf der Seite für die Kernkomponenten einen anderen Speicherort angeben. Stellen Sie jedoch sicher, dass dieser Speicherort den Netzwerkdienst ausführen kann. (Befehlszeilenoption: /installdir zum Festlegen eines nicht standardmäßigen Verzeichnisses)

### Für Kernkomponenten verwendete Features

Wählen Sie aus oder geben Sie an, ob Microsoft SQL Server Express installiert werden soll. Wenn Sie nicht mit den Datenbanken vertraut sind, lesen Sie den Artikel Datenbanken. (Befehlszeilenoption: /nosql zur Verhinderung der Installation)

Bei der Installation von Director wird die Microsoft-Remoteunterstützung automatisch installiert. Sie können wahlweise die Spiegelung in der Microsoft-Remoteunterstützung zur Verwendung mit der Director-Benutzerspiegelung aktivieren und TCP-Port 3389 öffnen. Dieses Feature ist standardmäßig aktiviert. (Befehlszeilenoption: /no_remote_assistance)

### Firewallports für Kernkomponenten

Standardmäßig werden die folgenden Ports automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Sie können diese Standardaktion deaktivieren und die Ports manuell öffnen, wenn Sie die Firewall eines Drittanbieters oder keine Firewall verwenden, oder wenn Sie die Ports selbst öffnen möchten. Vollständige Portinformationen zu diesem und anderen Citrix Produkten finden Sie unter CTX101810. (Befehlszeilenoption: /configure_firewall)

- Controller: TCP 80, 443
- Director: TCP 80, 443
- Lizenzserver: TCP 7279, 8082, 8083, 27000
- StoreFront: TCP 80, 443

# Leitfaden zur VDA-Installation

- Die VDA-Installationsprogramme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Informationen zu den unterstützten Betriebssystemen und zu den VDA-Versionen enthält der Artikel Systemanforderungen. Die meisten Komponentenvoraussetzungen werden automatisch installiert. Ausnahmen werden in dem Artikel aufgeführt. Wenn Sie einen VDA für Windows-Serverbetriebssysteme installieren, werden die Rollendienste für die Remotedesktopdienste automatisch installiert und aktiviert, wenn sie nicht bereits installiert und aktiviert sind.
- Wenn Sie einen VDA auf einer Maschine mit Windows 7 oder Windows Server 2008 R2 installieren, vergewissern Sie sich vor der VDA-Installation, dass .NET 3.5.1 installiert ist. Der Abschnitt Neustarts unten enthält zusätzliche Tipps zu den Installationsvoraussetzungen.
- Der Druckspoolerdienst ist auf den unterstützten Windows-Servern standardmäßig aktiviert. Ist dieser Dienst deaktiviert, können Sie keinen VDA für Windows-Serverbetriebssysteme installieren. Stellen Sie daher vor der VDA-Installation sicher, dass der Dienst aktiviert ist.
- Die Profilverwaltung wird automatisch bei der Installation von Virtual Desktop Agent installiert. Sie können sie zwar ausschließen, wenn Sie die Befehlszeilenschnittstelle verwenden, ein solcher Ausschluss wirkt sich jedoch auf Überwachung und Problembehandlung von VDAs mit Director aus.
- Wenn Sie VDA installieren, wird automatisch eine neue lokale Benutzergruppe namens "Benutzer mit direktem Zugriff" erstellt. Bei VDA für Windows-Desktopbetriebssysteme gilt diese Gruppe nur für RDP-Verbindungen; bei VDA für Windows-Serverbetriebssysteme gilt sie für ICA- und RDP-Verbindungen.
- Für Remote-PC-Zugriff-Konfigurationen ist VDA für Windows-Desktopbetriebssystem auf jedem physischen Büro-PC zu installieren, auf den die Benutzer zugreifen. Aktivieren Sie das Feature zum Optimieren nicht.
- Wenn Sie einen VDA auf einem Computer mit einem unterstützten Linux- Betriebssystem installieren möchten, konsultieren Sie den Artikel Installieren von VDAs unter Red Hat Linux bzw. Installieren von VDAs unter SUSE Linux. Diese enthalten wichtige Informationen.
- Der VDA benötigt gültige Controlleradressen für die Kommunikation, ansonsten können keine Sitzungen erstellt werden. Sie können Controlleradressen bei der Installation des VDAs oder später festlegen. Sie dürfen es nur nicht vergessen. Weitere Informationen finden Sie weiter unten im Abschnitt Delivery Controller-Adressen.
- Verwenden Sie nach der Installation eines VDAs für Serverbetriebssysteme unter Windows Server 2012 R2 das Tool zum Aktivieren von Kerberos (XASsonKerb.exe), um die ordnungsgemäße Funktion der Citrix Kerberos-Authentifizierung sicherzustellen. Das Tool ist im Ordner "Support > Tools>XASsonKerb" auf dem Installationsmedium. Für die Verwendung benötigen Sie lokale Administratorrechte. Führen Sie **xassonkerb.exe –install** über eine Eingabeaufforderung auf dem Server aus. Wenn Sie später ein Update ausführen, bei dem der Registrierungspfad HKLM\System\CurrentControlSet\Control\LSA\OSConfig geändert wird, führen Sie den Befehl noch einmal aus. Zum Anzeigen aller verfügbaren Tooloptionen führen Sie den Befehl mit dem Parameter –help aus.

### VDA-Installationsprogramme

Sie können VDAs über das Produktinstallationsprogramm oder das eigenständige Installationsprogramm installieren. Beide bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.

Das Produktinstallationsprogramm erkennt automatisch das Betriebssystem und erlaubt nur die Installation des für das System geeigneten Windows-VDA: VDA für Windows-Serverbetriebssysteme oder VDA für Windows-Desktopbetriebssysteme.

## Eigenständiges VDA-Installationspaket

Das kleinere, eigenständige Paket ist besser für Bereitstellungen auf physischen Computern oder an Remotestandorten geeignet, da es über Electronic Software Distribution (ESD)-Pakete als limitierte Bereitstellung oder lokale Kopie bereitgestellt wird. Das eigenständige Paket ist in erster Linie für Bereitstellungen über die Befehlszeile (unbeaufsichtigte Installation) gedacht, da die gleichen Befehlszeilenparameter wie beim Produktinstallationsprogramm verwendet werden.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Das Paket bietet zudem dieselbe grafische Oberfläche wie das Produktinstallationsprogramm.

Verwenden der grafischen Oberfläche des eigenständigen VDA-Installationsprogramms

Verwenden der Befehlszeilenschnittstelle des eigenständigen VDA-Installationsprogramms

Es gibt zwei selbstextrahierende eigenständige VDA-Installationspakete: eines zur Installation auf unterstützten Serverbetriebssystemmaschinen und eines für unterstützte Workstation- bzw. Desktopbetriebssystemmaschinen.

Standardmäßig werden die Dateien im Paket in den Ordner "Temp" extrahiert. Zum Extrahieren in den Ordner "Temp" wird auf der Maschine mehr Speicherplatz beansprucht, als wenn Sie das Produktinstallationsprogramm verwenden. Dateien, die in den Ordner "Temp" extrahiert wurden, werden nicht automatisch gelöscht, aber Sie können sie nach Abschluss der Installation manuell löschen (aus C:\Windows\Temp\Ctx-*, wobei * ein willkürlicher GUID ist). Alternativ können Sie den Befehl /extract mit einem absoluten Pfad verwenden.

Wenn in der Bereitstellung Microsoft System Center Configuration Manager verwendet wird, schlägt eine VDA-Installation u. U. scheinbar mit Exitcode 3 fehl, obwohl der VDA erfolgreich installiert wird. Sie können diese irreführende Meldung vermeiden, indem Sie die Installation mit einem CMD-Script umschließen oder die Erfolgscodes im Configuration Manager-Paket ändern. Weitere Informationen finden Sie in der Forumsdiskussion http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

### Neustarts beim Installieren eines VDAs

Bei der VDA-Installation ist zum Abschluss ein Neustart erforderlich.

Wenn Sie die Zahl der Neustarts während der Installation auf ein Minimum begrenzen möchten, gehen Sie folgendermaßen vor:

- Stellen Sie vor der VDA-Installation sicher, dass eine unterstützte .NET Framework-Version installiert ist.
- Installieren und aktivieren Sie auf Windows-Serverbetriebssystemmaschinen vor der VDA-Installation die Rollendienste für Remotedesktopdienste.

Andere Voraussetzungen erfordern normalerweise keine Neustarts, daher können Sie das Installationsprogramm einfach laufen lassen.

Wenn Sie vor der VDA-Installation nicht die Voraussetzungen installieren und dann die Option /noreboot für die Befehlszeileninstallation festlegen, müssen Sie die Neustarts ausführen. Wenn Sie beispielsweise die Voraussetzungen automatisch bereitstellen, wartet das Installationsprogramm nach der Installation von RDS auf einen Neustart. Führen Sie nach dem Neustart den Befehl erneut aus, damit die Installation des VDAs fortgesetzt wird.

### VDAs unter nicht unterstützten Windows-Betriebssystemen

Die aktuellen VDAs werden unter Windows XP und Windows Vista nicht unterstützt. Außerdem können einige Features in diesem und anderen neueren Releases unter diesen Betriebssystemen nicht verwendet werden. Citrix empfiehlt, die Sie solche Systeme durch derzeit unterstützte Windows-Desktopbetriebssystemversionen ersetzen und dann einen VDA aus diesem Release installieren. Wenn Maschinen mit Windows XP oder Windows Vista weiter betrieben werden müssen, können Sie auch eine ältere Virtual Desktop Agent-Version (5.6 FP1 mit bestimmten Hotfixes) installieren. Einzelheiten hierzu finden Sie unter CTX140941. Beachten Sie Folgendes:

- Die Kernkomponenten (Controller, Studio Director, StoreFront, Lizenzserver) können nicht auf einem Windows XP- oder Windows Vista-System installiert werden.
- Wenn Sie Windows XP oder Windows Vista verwenden und einen Maschinenkatalog mit solchen Maschinen erstellen,

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

müssen Sie auf der Seite "Masterimage" für "Wählen Sie die VDA-Version..." die Option "5.6 FP1" auswählen.
- Remote-PC-Zugriff wird auf Windows Vista-Systemen nicht unterstützt.
- Citrix Support für Windows XP endete zusammen mit dem erweiterten Support von Microsoft am 8. April 2014.
- Die Verwendung älterer VDAs kann sich auf die Verfügbarkeit von Features und die Registrierung des VDAs beim Controller auswirken (siehe auch Hinweise zu heterogenen Umgebungen).

# Angaben bei der VDA-Installation

In den folgenden Abschnitten werden die Parameter erläutert, die Sie bei der Installation festlegen. Die Beschreibung folgt den Schritten des Assistenten der grafischen Oberfläche; entsprechende Optionen für die Befehlszeilenschnittstelle werden ebenfalls aufgeführt. In den Artikeln zur Installation wird erläutert, wie Sie den Assistenten starten bzw. Befehle mit Optionen eingeben.

Der Artikel Leitfaden zur VDA-Installation enthält Informationen zu Aufgaben, die ggf. nach einer VDA-Installation erforderlich sind.

## Umgebung

Die VDA-Umgebung gibt vor, wie der VDA verwendet wird:

- Die Standardoption "Masterimage" gibt an, dass Sie mit den Maschinenerstellungsdiensten (MCS) oder Provisioning Services virtuelle Maschinen basierend auf einem Masterimage in einem Hypervisor oder Clouddienst erstellen. Sie installieren den VDA auf dem Masterimage. (Befehlszeilenoption /masterimage)
- Die Option "Remote-PC-Zugriff" gibt an, dass Sie den VDA auf einer physischen Maschine oder auf einer VM ohne VDA installieren.

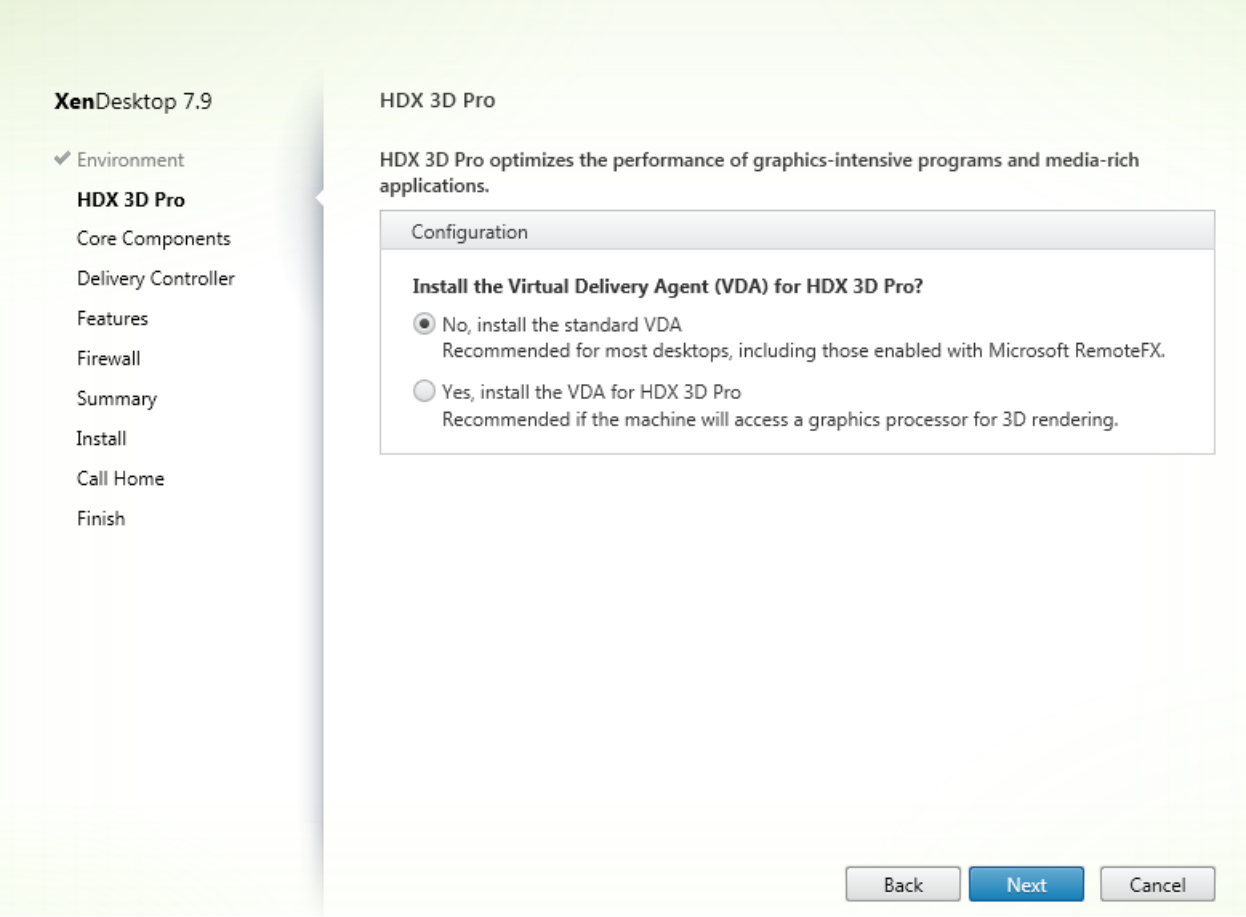
> **Important**
>
> Verwenden Sie die Befehlszeile in XenApp und XenDesktop 7.9 nur für Remote-PC-Zugriff-Bereitstellungen. Weitere Informationen finden Sie unter Installieren an der Befehlszeile und Bekannte Probleme [#637741].

## HDX 3D Pro (VDA für Windows-Desktopbetriebssysteme)

Wenn Sie einen VDA über die grafische Benutzeroberfläche installieren, wird diese Seite nur angezeigt, wenn Sie einen VDA auf einer Desktopbetriebssystemmaschine (nicht auf einer Serverbetriebssystemmaschine) installieren. Konfigurieren Sie den VDA für den Standardmodus oder den HDX 3D Pro-Modus.

- Der VDA-Standardmodus wird für die meisten Desktops empfohlen, einschließlich solcher mit aktiviertem Microsoft RemoteFX. Dieser Modus ist standardmäßig aktiviert.
- Ein VDA im HDX 3D Pro-Modus dient zur Optimierung der Leistung grafikintensiver Programme und Anwendungen sowie Anwendungen mit hohem Multimedia-Anteil. Er wird empfohlen, wenn die Maschine zur 3D-Wiedergabe auf einen Grafikprozessor zugreift. (Die Befehlszeilenoption ist nur auf Desktopbetriebssystemmaschinen gültig: /enable_hdx_3d_pro)


© 1999-2017 Citrix Systems, Inc. All rights reserved.




| Standard-VDA | VDA für HDX 3D Pro |
|---|---|
| • Im Allgemeinen am besten für virtuelle Desktops ohne Grafikhardwarebeschleunigung und für Remote-PC-Zugriff geeignet.<br>• Unterstützt die GPU-Beschleunigung mit allen GPUs, wobei einige Einschränkungen aufgrund von Anwendungskompatibilität gelten:<br>  • Unter Windows 7, 8 und 8.1 ist GPU-Beschleunigung für DirectX-Featureebenen bis 9.3 möglich. Einige DirectX 10, 11, 12-Anwendungen können u. U. nicht ausgeführt werden, wenn sie kein Fallback auf DirectX 9 tolerieren.<br>  • Unter Windows 10 ist GPU-Beschleunigung auf DirectX 10, 11 und 12-Anwendungen beschränkt, die im Fenstermodus (nicht im Vollbildmodus) angezeigt werden. DirectX 9 und Vollbildanwendungen werden durch Software-Rendering (WARP) wiedergegeben.<br>  • OpenGL-Anwendungsbeschleunigung in Remotesitzungen, wenn vom GPU-Hersteller unterstützt (derzeit nur NVIDIA). | • Im Allgemeinen am besten geeignet für Desktops in Datencentern mit Grafikhardwarebeschleunigung, wenn nicht mehr als vier Monitore benötigt werden.<br>• Unterstützt die GPU-Beschleunigung mit allen GPUs; das Ausblenden der Konsole, nicht standardmäßige Bildschirmauflösungen und echte Unterstützung für mehrere Bildschirme erfordern jedoch NVIDIA GRID oder Intel Iris Pro Graphics.<br>• Verwendet den Grafiktreiber des Herstellers, der die umfassendste Anwendungskompatibilität bietet.<br>  • Alle 3D-APIs (DirectX oder OpenGL), die die GPU unterstützt.<br>  • Unterstützung für Vollbild-3D-App mit Intel Iris Pro (nur Windows 10) und NVIDIA GRID.<br>  • Unterstützung für benutzerdefinierte Treibererweiterungen und APIs. Beispiel: CUDA oder OpenCL.<br>• Unterstützt bis zu vier Monitore. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| • Verwendet den Citrix WDDM-Anzeigetreiber, der beliebige Monitorauflösungen (bis zu 4K) und bis zu 8 Monitore unterstützt.<br>• Desktopgestaltungsumleitung als Option für Breitbandzugriff auf Aero-Desktops mit Windows 7 und 8.x.<br>  • Windows-Desktopgestaltung wird auf das Benutzergerät (Windows oder Mac) verlagert. | |

**Remote-PC-Zugriff und HDX 3D Pro-Modus**

Für Remote-PC-Zugriff ist der VDA normalerweise mit der standardmäßigen VDA-Option konfiguriert. Für Remote-PC-Zugriff, der mit HDX 3D Pro konfiguriert ist, wird das Ausblenden des Bildschirms für Intel Iris Pro Graphics und Intel HD Graphics 5300 und höher unterstützt (Intel Core-Prozessoren der 5. Generationund Intel Core i5-Prozessoren der 6. Generation) sowie für NVIDIA Quadro- und NVIDIA GRID-GPUs.

## Kernkomponenten (Installationsort und Installation von Citrix Receiver)

VDAs werden standardmäßig unter C:\Programme\Citrix installiert. Sie können einen anderen Speicherort während der Installation angeben. Stellen Sie jedoch sicher, dass dieser Speicherort den Netzwerkdienst ausführen kann. (Befehlszeilenoption: /installdir zum Festlegen eines nicht standardmäßigen Verzeichnisses)

Standardmäßig wird Citrix Receiver für Windows mit dem VDA installiert. Sie können diese Standardaktion deaktivieren. (Befehlszeilenoption: /components vda, um die Installation von Citrix Receiver zu verhindern)

## Delivery Controller

Sie können die Adressen (FQDNs) der installierten Controller bei der Installation des VDAs festlegen (empfohlen) oder zu einem späteren Zeitpunkt. Sie müssen zwar keine Controlleradressen bei der Installation eines VDAs angeben, ein VDA kann sich jedoch ohne diese Angabe nicht bei einem Controller registrieren. Wenn VDAs sich nicht registrieren können, können Benutzer auf Maschinen mit diesen VDAs nicht auf ihre Desktops und Anwendungen zugreifen. (Befehlszeilenoption: /controllers)

- Wenn Sie Controller-FQDNs bei der VDA-Installation angeben, wird versucht, eine Verbindung mit diesen Adressen herzustellen. Schlägt dies fehl, werden Informationsmeldungen angezeigt.
- Wenn Sie angeben, dass Sie Controlleradressen später festlegen möchten, werden Sie vom Installationsprogramm entsprechend erinnert. Wenn Sie einen VDA ohne Angabe einer Controlleradresse installieren, können Sie entweder das Installationsprogramm zu einem späteren Zeitpunkt erneut ausführen oder die Citrix Gruppenrichtlinie verwenden.

Wenn Sie Controlleradressen bei der VDA-Installation und in der Gruppenrichtlinie festlegen, haben die Richtlinieneinstellungen Vorrang vor den bei der Installation festgelegten Einstellungen.

Vergessen Sie nicht, dass zur VDA-Registrierung außerdem die Firewallports für die Kommunikation mit einem Controller geöffnet sein müssen.

Nach der ersten Angabe von Controlleradressen bei der VDA-Installation oder zu einem späteren Zeitpunkt können Sie das Feature für automatische Updates zum Aktualisieren von VDAs verwenden, wenn weitere Controller installiert werden.

Weitere Informationen dazu, wie VDAs Controller erkennen und sich dort registrieren, finden Sie im Artikel Delivery Controller.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Feature

Sie können folgende Features für VDAs aktivieren oder deaktivieren:

- **Leistung optimieren:** Wenn diese Funktion aktiviert ist, wird das Optimierungstool für VDAs verwendet, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Weitere Informationen finden Sie unter CTX125874. Aktivieren Sie diese Option nicht, wenn Sie Remote-PC-Zugriff verwenden möchten. (Befehlszeilenoption: /optimize)
- **Windows-Remoteunterstützung verwenden:** Wenn dieses Feature aktiviert ist, wird die Microsoft-Remoteunterstützung mit dem Feature zur Benutzerspiegelung von Director verwendet, und Windows öffnet automatisch TCP-Port 3389 in der Firewall, selbst wenn Sie die Firewallports normalerweise manuell öffnen. Die Funktion ist standardmäßig aktiviert. (Befehlszeilenoption: /enable_remote_assistance)
- **Echtzeitaudioübertragung für Audio verwenden:** Wenn dieses Feature aktiviert ist, wird UDP für Audiopakete verwendet, wodurch die Audioleistung verbessert werden kann. Die Funktion ist standardmäßig aktiviert. (Befehlszeilenoption: /enable_real_time_transport)
- **Framehawk:** (Standardeinstellung=aktiviert) Wenn dieses Feature aktiviert ist, werden die bidirektionalen UDP-Ports 3224-3324 geöffnet. (Sie können den Portbereich später in der Citrix Richtlinieneinstellung für den Framehawk-Anzeigekanal ändern. Dazu müssen Sie lokale Firewallports öffnen.) Ein UDP-Netzwerkpfad muss in jeder internen Firewall (VDA an Citrix Receiver oder VDA an NetScaler Gateway) und jeder externen Firewall (NetScaler Gateway an Citrix Receiver) geöffnet sein. Wenn Sie NetScaler Gateway bereitstellen, werden Framehawk-Datagramme mit DTLS verschlüsselt (Standard-UDP-Port 443). Weitere Informationen finden Sie in dem Artikel Framehawk. (Befehlszeilenoption: /enable_framehawk_port)
- **Citrix App-V-Veröffentlichungskomponenten installieren:** (standardmäßig aktiviert) Aktivieren Sie dieses Feature, wenn Sie Anwendungen aus Paketen auf App-V-Servern verwenden möchten. Weitere Informationen finden Sie im Artikel App-V. (Befehlszeilenoption /no_appv verhindert die Komponenteninstallation)
- **Personal vDisk:** Wenn dieses Feature aktiviert ist, können persönliche vDisks mit einem Masterimage verwendet werden. Die Funktion ist standardmäßig deaktiviert und steht bei Installation eines VDAs für Desktopbetriebssysteme auf einer VM zur Verfügung. Weitere Informationen finden Sie im Artikel Personal vDisks. (Befehlszeilenoption: /baseimage)

## Firewall

Standardmäßig werden die folgenden Ports automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Sie können diese Standardaktion deaktivieren und die Ports manuell öffnen, wenn Sie die Firewall eines Drittanbieters oder keine Firewall verwenden, oder wenn Sie die Ports selbst öffnen möchten. Vollständige Portinformationen finden Sie unter CTX101810. (Befehlszeilenoption: /enable_hdx_ports)

- Controllerkommunikation: TCP 80, 1494, 2598, 8008. Für die Kommunikation zwischen Benutzergeräten und virtuellen Desktops müssen Sie eingehendes TCP auf Ports 1494 und 2598 als Portausnahmen konfigurieren. Aus Sicherheitsgründen empfiehlt Citrix, diese registrierten Ports ausschließlich für das ICA-Protokoll und das Common Gateway Protocol zu verwenden. Für die Kommunikation zwischen Controller und virtuellen Desktops müssen Sie den eingehenden Port 80 als Portausnahme konfigurieren.
- Remoteunterstützung: TCP 3389. Windows öffnet diesen Port automatisch, wenn die Remoteunterstützung auf der vorherigen Seite aktiviert wird, selbst wenn Sie festlegen, dass Sie die Ports manuell öffnen.
- Echtzeitaudioübertragung: UDP 16500-16509.
- Framehawk: UDP 3224-3324.

## Zusammenfassung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nachdem Sie die Angaben überprüft und auf **Installieren** geklickt haben, wird der Installationsfortschritt angezeigt. Nach Abschluss der Installation ist ein Neustart der Maschine erforderlich, bevor der VDA verwendet werden kann.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# VMware-Virtualisierungsumgebungen

Jul 08, 2016

Folgen Sie diesen Anweisungen, wenn Sie zur Bereitstellung von virtuellen Maschinen VMware verwenden.

# Installieren und Konfigurieren des Hypervisors

**Schritt 1**: Installieren Sie vCenter Server und die Verwaltungstools. (Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.)

**Schritt 2**: Erstellen Sie ein VMware-Benutzerkonto mit den folgenden Mindestberechtigungen auf DataCenter-Ebene. Dieses Konto verfügt über Berechtigungen zum Erstellen neuer VMs und wird verwendet, um mit vCenter zu kommunizieren.

| SDK | Benutzeroberfläche |
|---|---|
| Datastore.AllocateSpace | Datastore > Allocate space |
| Datastore.Browse | Datastore > Browse datastore |
| Datastore.FileManagement | Datastore > Low level file operations |
| Network.Assign | Network > Assign network |
| Resource.AssignVMToPool | Resource > Assign virtual machine to resource pool |
| System.Anonymous, System.Read und System.View | Automatisch hinzugefügt. |
| Task.Create | Tasks > Create task |
| VirtualMachine.Config.AddRemoveDevice | Virtual machine > Configuration > Add or remove device |
| VirtualMachine.Config.AddExistingDisk | Virtual machine > Configuration > Add existing disk |
| VirtualMachine.Config.AddNewDisk | Virtual machine > Configuration > Add new disk |
| VirtualMachine.Config.AdvancedConfig | Virtual machine > Configuration > Advanced |
| VirtualMachine.Config.CPUCount | Virtual machine > Configuration > Change CPU Count |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| VirtualMachine.Config.Memory | Virtual machine > Configuration > Memory |
| VirtualMachine.Config.RemoveDisk | Virtual machine > Configuration > Remove disk |
| VirtualMachine.Config.Resource | Virtual machine > Configuration > Change resource |
| VirtualMachine.Config.Settings | Virtual machine > Configuration > Settings |
| VirtualMachine.Interact.PowerOff | Virtual machine > Interaction > Power Off |
| VirtualMachine.Interact.PowerOn | Virtual machine > Interaction > Power On |
| VirtualMachine.Interact.Reset | Virtual machine > Interaction > Reset |
| VirtualMachine.Interact.Suspend | Virtual machine > Interaction > Suspend |
| VirtualMachine.Inventory.Create | Virtual machine > Inventory > Create new |
| VirtualMachine.Inventory.CreateFromExisting | Virtual machine > Inventory > Create from existing |
| VirtualMachine.Inventory.Delete | Virtual machine > Inventory > Remove |
| VirtualMachine.Inventory.Register | Virtual machine > Inventory > Register |
| VirtualMachine.Provisioning.Clone | Virtual machine > Provisioning > Clone virtual machine |
| VirtualMachine.Provisioning.CloneTemplate | Virtual machine > Provisioning > Clone template |
| VirtualMachine.Provisioning.DiskRandomAccess | Virtual machine > Provisioning > Allow disk access |
| VirtualMachine.Provisioning.GetVmFiles | Virtual machine > Provisioning > Allow virtual machine download |
| VirtualMachine.Provisioning.PutVmFiles | Virtual machine > Provisioning > Allow virtual machine files upload |
| VirtualMachine.Provisioning.DeployTemplate | Virtual machine > Provisioning > Deploy template |
| VirtualMachine.Provisioning.MarkAsVM | Virtual machine > Provisioning > Mark as virtual machine |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| VirtualMachine.State.CreateSnapshot | vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Create snapshot<br><br>vSphere 5.5: Virtual machine > Snapshot management > Create snapshot |
| VirtualMachine.State.RemoveSnapshot | vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Remove snapshot<br><br>vSphere 5.5: Virtual machine > Snapshot management > Remove snapshot |
| VirtualMachine.State.RevertToSnapshot | vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Revert to snapshot<br><br>vSphere 5.5: Virtual machine > Snapshot management > Revert to snapshot |

**Schritt 3:** Wenn Sie die erstellten VMs mit Tags kennzeichnen wollen, fügen Sie die folgenden Berechtigungen dem Benutzerkonto hinzu:

| SDK | Benutzeroberfläche |
|---|---|
| Global.ManageCustomFields | Global > Manage custom attributes |
| Global.SetCustomField | Global > Set custom attribute |

Um sicherzustellen, dass Sie ein sauberes Basisimage zum Erstellen neuer VMs verwenden, fügen Sie Tags den VMs hinzu, die mit den Maschinenerstellungsdiensten erstellt wurden. Damit schließen Sie sie aus der Liste der für Basisimages verfügbaren virtuellen Maschinen aus.

**Schritt 4**: Zum Erstellen von AppDisks muss das Benutzerkonto die folgenden zusätzlichen Berechtigungen haben:

- SDK: VirtualMachine.Config.EditDevice
- Benutzeroberfläche: Virtual machine > Configuration > Modify Device Settings

# Beschaffen und Importieren eines Zertifikats

Um die vSphere-Kommunikation zu schützen, empfiehlt Citrix die Verwendung von HTTPS statt HTTP. HTTPS benötigt digitale Zertifikate. Citrix empfiehlt die Verwendung eines digitalen Zertifikats, das von einer Zertifizierungsstelle unter Berücksichtigung der Sicherheitsrichtlinie Ihrer Organisation erstellt wurde.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Sie kein digitales Zertifikat verwenden können, das von einer Zertifizierungsstelle ausgestellt wurde, können Sie das mit VMware installierte selbstsignierte Zertifikat verwenden, vorausgesetzt, die Sicherheitsrichtlinie Ihrer Organisation lässt dies zu. Fügen Sie das VMware vCenter-Zertifikat jedem Controller hinzu. Führen Sie diese Schritte aus:

1. Fügen Sie den vollqualifizierten Domänennamen (FQDN) des Computers, auf dem vCenter Server ausgeführt wird, der Hostdatei auf dem Server im Verzeichnis %SystemRoot%/WINDOWS/system32/Drivers/etc/ hinzu. Dieser Schritt ist nur erforderlich, wenn der FQDN des Computers, auf dem vCenter Server ausgeführt wird, nicht bereits im Domänennamensystem vorhanden ist.
2. Rufen Sie das vCenter-Zertifikat mit einer der folgenden Methoden ab:
   - Führen Sie auf dem vCenter-Server folgende Schritte aus:
     1. Kopieren Sie die Datei rui.crt vom vCenter-Server zu einem Speicherort, auf den Ihre Delivery Controller zugreifen können.
     2. Navigieren Sie auf dem Controller zu dem Speicherort des exportierten Zertifikats und öffnen Sie die Datei rui.crt.
   - Laden Sie das Zertifikat über einen Webbrowser herunter. Bei Verwendung von Internet Explorer müssen Sie (abhängig von Ihrem Benutzerkonto) ggf. in Internet Explorer mit der rechten Maustaste klicken und "Als Administrator ausführen" wählen, um das Zertifikat herunterzuladen und zu installieren.
     1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung zu dem vCenter-Server her, z. B. https://server1.domain1.com
     2. Akzeptieren Sie die Sicherheitswarnungen.
     3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
     4. Zeigen Sie das Zertifikat an und klicken Sie auf die Registerkarte Details.
     5. Wählen Sie "In Datei kopieren" und exportieren Sie im CER-Format; geben Sie an entsprechender Stelle einen Namen an.
     6. Speichern Sie das exportierte Zertifikat.
     7. Navigieren Sie auf den Speicherort des exportierten Zertifikats und öffnen Sie die CER-Datei.
   - Direkter Import von Internet Explorer, der als Administrator ausgeführt wird:
     1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her, z. B. https://server1.domain1.com.
     2. Akzeptieren Sie die Sicherheitswarnungen.
     3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
     4. Zeigen Sie das Zertifikat an.
   - Importieren des Zertifikats auf jedem Controller in den Zertifikatspeicher:
     1. Klicken Sie auf "Zertifikat installieren", wählen Sie "Lokaler Computer" aus und klicken Sie dann auf "Weiter".
     2. Wählen Sie "Alle Zertifikate in folgendem Speicher speichern" aus und klicken Sie dann auf "Durchsuchen".
     3. Bei Verwendung von Windows Server 2008 R2:
        1. Aktivieren Sie das Kontrollkästchen "Physischen Speicher anzeigen".
        2. Erweitern Sie Vertrauenswürdige Personen.
        3. Wählen Sie "Lokaler Computer".
        4. Klicken Sie auf "Weiter" und dann auf "Fertig stellen".

        Bei Verwendung von Windows Server 2012 oder Windows Server 2012 R2:

        1. Wählen Sie "Vertrauenswürdige Personen" und klicken Sie auf "OK".
        2. Klicken Sie auf "Weiter" und dann auf "Fertig stellen".

   Wichtig: Wenn Sie den Namen des vSphere-Servers nach der Installation ändern, müssen Sie ein neues selbstsigniertes Zertifikat auf diesem Server erstellen, bevor Sie das neue Zertifikat importieren.

## Erstellen einer Master-VM


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verwenden Sie eine Master-VM zur Bereitstellung von Benutzerdesktops und Anwendungen. Auf dem Hypervisor

1. Installieren Sie einen VDA auf der Master-VM unter Auswahl der Option zur Desktopoptimierung, wodurch die Leistung verbessert wird.
2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Sicherungskopie zu verwenden.

### Erstellen virtueller Desktops

Wenn Sie VM mit Studio erstellen statt einen vorhandenen Maschinenkatalog auszuwählen, geben Sie beim Einrichten der Hostinginfrastruktur für die Erstellung virtueller Desktops die folgenden Informationen ein:

1. Wählen Sie den VMware vSphere-Hosttyp aus.
2. Geben Sie die Adresse des Zugriffspunkts für das vCenter SDK ein.
3. Geben Sie die Anmeldeinformationen für das zuvor eingerichtete VMware-Konto ein, das Berechtigungen zum Erstellen neuer VMs hat. Geben Sie den Benutzernamen im Format Domäne/Benutzername ein.

# VMware SSL-Fingerabdruck

Mit dem VMware SSL-Fingerabdruckfeature wurde ein häufig aufgetretener Fehler beim Erstellen einer Hostverbindung mit einem VMware vSphere-Hypervisor behoben. Bisher musste der Administrator eine Vertrauensstellung zwischen den Site-Delivery Controllern und dem Hypervisor-Zertifikat vor dem Erstellen einer Verbindung manuell erstellen. Dank VMware SSL-Fingerabdruck ist dies nicht mehr nötig. Der Fingerabdruck des nicht vertrauenswürdigen Zertifikats wird in der Sitedatenbank gespeichert, damit der Hypervisor zwar nicht von den Controllern, jedoch von XenApp bzw. XenDesktop immer als vertrauenswürdig eingestuft wird.

Beim Erstellen einer vSphere-Hostverbindung in Studio wird ein Dialogfeld mit dem Zertifikat der Maschine angezeigt, mit der Sie eine Verbindung herstellen. Sie können dann wählen, ob sie als vertrauenswürdig gelten soll.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Microsoft System Center Virtual Machine Manager-Umgebungen

Jul 15, 2016

Befolgen Sie die nachfolgenden Anweisungen, wenn Sie Hyper-V mit Microsoft System Center Virtual Machine Manager (VMM) zur Bereitstellung von virtuellen Maschinen verwenden.

Dieses Release unterstützt Folgendes:

- VMM 2012: Bietet bessere Verwaltungsfunktionen und ermöglicht die Verwaltung des gesamten virtualisierten Datencenters sowie der virtuellen Maschinen. Dieses Release organisiert das Patchen von Clusterhosts sowie die Integration mit Windows Server Update Services und ermöglicht somit das Erstellen eines Basisplans für Patches, die jeder Host benötigt.
- VMM 2012 SP1: Bietet Leistungsverbesserungen für Maschinenerstellungsdienste (MCS), wenn Sie SMB 3.0 auf Dateiservern mit freigegebenen Clustervolumes und Storage Area Networks (SANs) verwenden. Diese Dateifreigaben bieten kostengünstiges Zwischenspeichern und reduzierte E/A im SAN-Speicher mit verbesserter Leistung.
- VMM 2012 R2: Ermöglicht die angemessene Verwaltung von wichtigen Windows Server 2012 R2-Funktionen, wie das Ausführen von VM-Snapshots, dynamische VHDX-Größenanpassung und Speicherplätze.

Dieses Release unterstützt nur virtuelle Maschinen der ersten Generation mit VMM 2012 R2. Mit MCS erstellte VM der zweiten Generation erscheinen nicht in der Auswahlliste für eine Master-VM. Auf ihnen ist der sichere Start standardmäßig aktiviert, wodurch eine richtige Funktionsweise des VDAs verhindert wird.

## Aktualisieren von VMM

- Upgrade von VMM 2012 auf VMM 2012 SP1 oder VMM 2012 R2
  Informationen zu den Anforderungen von VMM- und Hyper-V-Hosts finden Sie unter http://technet.microsoft.com/en-us/library/gg610649.aspx. Informationen zu den Anforderungen für die VMM-Konsole finden Sie unter http://technet.microsoft.com/en-us/library/gg610640.aspx.

  Ein gemischter Hyper-V-Cluster wird nicht unterstützt. Ein gemischter Cluster ist beispielsweise einer, bei dem eine Hälfte des Clusters Hyper-V 2008 und die andere Hälfte Hyper-V 2012 ausführen.

- Upgrade von VMM 2008 R2 auf VMM 2012 SP1
  Wenn Sie ein Upgrade von XenDesktop 5.6 unter VMM 2008 R2 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:
  1. Upgrade von VMM auf 2012 (jetzt XenDesktop 5.6 und VMM 2012)
  2. Upgrade von XenDesktop auf die aktuelle Version (jetzt aktuelle XenDesktop-Version und VMM 2012)
  3. Upgrade von VMM von 2012 auf 2012 SP1 (jetzt aktuelle XenDesktop-Version und VMM 2012 SP1)
- Upgrade von VMM 2012 SP1 auf VMM 2012 R2
  Wenn Sie ein Upgrade von XenDesktop oder XenApp 7 unter VMM 2012 SP1 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:
  1. Upgrade von XenDesktop oder XenApp auf die aktuelle Version (jetzt aktuelle XenDesktop-/XenApp-Version und VMM 2012 SP1)
  2. Upgrade von VMM 2012 SP1 auf 2012 R2 (jetzt aktuelle XenDesktop- oder XenApp-Version und VMM 2012 R2)

## Zusammenfassung von Installation und Konfiguration

1. Installieren und konfigurieren Sie einen Hypervisor.
   1. Installieren Sie Microsoft Hyper-V Server und VMM auf Ihren Servern. Alle Delivery Controller müssen in derselben Gesamtstruktur sein wie die VMM-Server.
   2. Installieren Sie die System Center VMM-Konsole auf allen Controllern.
   3. Überprüfen Sie die folgenden Kontoinformationen:
      - Das Konto, das Sie zum Festlegen von Hosts in Studio verwenden, ist ein VMM-Administrator oder delegierter VMM-Administrator für die relevanten Hyper-V-Maschinen. Wenn dieses Konto nur über die delegierte Administratorrolle in VMM verfügt, werden die Speicherdaten in Studio beim Erstellen des Hosts nicht aufgeführt.
      - Das Benutzerkonto, das für die Studio-Integration verwendet wird, muss auch Mitglied der lokalen Administratorsicherheitsgruppe auf jedem Hyper-V-Server sein, um zur Lebenszyklusverwaltung von VM (z. B. VM erstellen, aktualisieren und löschen) berechtigt zu sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Die direkte Installation eines Controllers auf einem Server, auf dem Hyper-V ausgeführt wird, wird nicht unterstützt.

2. Erstellen Sie eine Master-VM.
   1. Installieren Sie einen Virtual Delivery Agent auf der Master-VM und wählen Sie die Option zur Desktopoptimierung aus. Dies verbessert die Leistung.
   2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Sicherungskopie zu verwenden.
3. Erstellen Sie virtuelle Desktops. Bei Verwendung von MCS zum Erstellen von VM beim Erstellen einer Site oder einer Verbindung:
   1. Wählen Sie den Typ des Microsoft-Virtualisierungshosts aus.
   2. Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
   3. Geben Sie die Anmeldeinformationen für das zuvor erstellte Administratorkonto ein, das Berechtigungen zum Erstellen von neuen VMs enthält.
   4. Wählen Sie im Dialogfeld Hostdetails den Cluster oder eigenständigen Host aus, der beim Erstellen der neuen VMs verwendet werden soll. Wichtig: Sie müssen auch dann zu einem Cluster oder eigenständigen Host navigieren und diesen auswählen, wenn Sie eine Bereitstellung mit einem einzelnen Hyper-V-Host verwenden.

### MCS auf SMB 3-Dateifreigaben

Bei Maschinenkatalogen, die mit MSC auf SMB 3-Dateifreigaben für VM-Speicher erstellt wurden, müssen Sie darauf achten, dass die Anmeldeinformationen die nachfolgenden Anforderungen erfüllen, damit Aufrufe von der Hypervisor Communications Library (HCL) des Controllers die Verbindung mit dem SMB-Speicher herstellen:

- Die VMM-Benutzeranmeldeinformationen müssen vollständigen Lese-/Schreibzugriff auf den SMB-Speicher umfassen.
- Speichervorgänge auf dem virtuellen Datenträger werden bei Vorgängen im Lebenszyklus der VM über den Hyper-V-Server mit den VMM-Anmeldeinformationen durchgeführt.

Wenn Sie SMB als Speicher verwenden, aktivieren Sie das Feature "CredSSP" (Credential Security Support Provider) vom Controller auf den einzelnen Hyper-V-Maschinen, wenn Sie VMM 2012 SP1 mit Hyper-V unter Windows Server 2012 verwenden. Weitere Informationen finden Sie unter CTX137465.

Über eine standardmäßige Remote-PowerShell V3-Sitzung verwendet die HCL CredSSP zum Öffnen einer Verbindung mit der Hyper-V-Maschine. Dieses Feature übergibt mit Kerberos verschlüsselte Benutzeranmeldeinformationen an die Hyper-V-Maschine. Die PowerShell-Befehle in dieser Sitzung auf der Remotemaschine mit Hyper-V werden dann unter Verwendung der angegebenen Anmeldeinformationen (in diesem Fall, derer des VMM-Benutzers) ausgeführt, sodass eine ordnungsgemäße Kommunikation mit dem Speicher gewährleistet wird.

Die folgenden Tasks verwenden PowerShell-Skripts der HCL, die an die Hyper-V-Maschine zur Verwendung mit SMB 3.0-Speicher gesendet werden.

- **Konsolidieren des Masterimages**: Ein Masterimage erstellt ein neues MCS-Provisioningschema (Maschinenkatalog). Die Master-VM wird durch dieses Schema geklont und vereinfacht, damit sie zum Erstellen neuer VM aus dem neu erstellten Datenträger bereit ist (die Abhängigkeit zur ursprünglichen Master-VM wird entfernt).
  ConvertVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:
  ```
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext) $result
  ```
- **Erstellen eines differenzierenden Datenträgers**: erstellt einen differenzierenden Datenträger aus dem Masterimage, das durch Konsolidierung des Masterimages generiert wurde. Der differenzierende Datenträger wird dann an eine neue VM angeschlossen.
  CreateVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:
  ```
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.CreateVirtualHardDisk($vhdastext); $result
  ```
- **Upload von Identitätsdisks**: Von der HCL kann die Identitätsdisk nicht direkt in den SMB-Speicher hochgeladen werden. Daher muss die Identitätsdisk von der Hyper-V-Maschine hochgeladen und in den Speicher kopiert werden. Da die Hyper-V-Maschine die Disk nicht auf dem Controller lesen kann, muss sie von der HCL zuerst wie folgt über die Hyper-V-Maschine kopiert werden:
  1. Upload der Identitätsdisk durch die HCL auf die Hyper-V-Maschine über die Administratorfreigabe.
  2. Die Disk wird von der Hyper-V-Maschine über ein PowerShell-Skript, das in der Remote-PowerShell-Sitzung ausgeführt wird, in den SMB-Speicher kopiert. Auf der Hyper-V-Maschine wird ein Ordner erstellt, dessen Berechtigungen nur für den VMM-Benutzer gesperrt sind (über die remote PowerShell-Verbindung).
  3. Die HCL löscht die Datei aus der Administratorfreigabe.
  4. Wenn der Identitätsdisk-Upload durch die HCL auf die Hyper-V-Maschine abgeschlossen ist, werden die Identitätsdisks von der Remote-PowerShell-Sitzung in den SMB-Speicher kopiert und dann aus der Hyper-V-Maschine gelöscht.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Falls der Ordner der Identitätsdisk gelöscht wird, wird er neu erstellt, damit er zur Wiederverwendung verfügbar ist.

- **Download von Identitätsdisks**: Wie beim Upload wird die Identitätsdisk über die Hyper-V-Maschine an die HCL übergeben. Beim folgenden Prozess wird, falls noch nicht vorhanden, ein Ordner erstellt, der nur VMM-Benutzerbenutzerberechtigungen auf dem Hyper-V-Server hat.
  1. Die Disk wird von der Hyper-V-Maschine aus dem SMB-Speicher in den lokalen Hyper-V-Speicher kopiert, und zwar über ein PowerShell-Skript, das in der Remote-PowerShell V3-Sitzung ausgeführt wird.
  2. Die HCL liest die Disk aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.
  3. Die HCL löscht die Datei aus der Administratorfreigabe.
- **Erstellen einer persönlichen vDisk**: Wenn der Administrator die VM in einem Personal vDisk-Maschinenkatalog erstellt, muss eine leere Disk (PvD) erstellt werden.

  Der Aufruf zum Erstellen einer leeren Disk erfordert keinen direkten Zugriff auf den Speicher. Wenn Sie PvDs auf anderen Speichern als dem Haupt- oder dem Betriebssystemdatenträger haben, verwenden Sie Remote-PowerShell zum Erstellen der PvD in einem Ordner mit dem gleichen Namen wie die VM, aus dem sie erstellt wurde. Verwenden Sie Remote-PowerShell nicht mit CSV oder LocalStorage. VMM-Befehlsfehler werden vermieden, wenn zuerst das Verzeichnis und dann die leere Disk erstellt werden.

  Führen Sie auf der Hyper-V-Maschine mkdir an dem Speicher aus.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Microsoft Azure-Virtualisierungsumgebungen

Jul 08, 2016

# Verbindungskonfiguration

Wenn Sie Studio zum Erstellen einer Microsoft Azure-Verbindung verwenden, benötigen Sie Informationen aus der Datei mit den Veröffentlichungseinstellungen von Microsoft Azure. Die Informationen in dieser XML-Datei für die einzelnen Abonnements sehen in etwa folgendermaßen aus (das tatsächliche Verwaltungszertifikat ist viel länger):

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl; sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

Bei dem folgenden Verfahren wird davon ausgegangen, dass Sie eine Verbindung mithilfe von Studio erstellen und entweder den Assistenten für die Siteerstellung oder den Assistenten für die Verbindungserstellung gestartet haben.

1. Rufen Sie in einem Browser https://manage.windowsazure.com/publishsettings/index auf.
2. Laden Sie die Datei mit den Veröffentlichungseinstellungen herunter.
3. Klicken Sie in Studio auf der Seite **Verbindung** des Assistenten nach Auswahl des Verbindungstyps "Microsoft Azure" auf "Importieren".
4. Wenn Sie mehrere Abonnements haben, werden Sie zur Auswahl des gewünschten Abonnements aufgefordert.

ID und Zertifikat werden automatisch und ohne Benutzereingriff in Studio importiert.

Energieaktionen, für die eine Verbindung verwendet wird, unterliegen Schwellenwerten. Im Allgemeinen sind die Standardwerte geeignet und sollten nicht geändert werden. Sie können sie jedoch beim Bearbeiten einer Verbindung ändern (beim Erstellen von Verbindungen können diese Werte nicht geändert werden). Weitere Informationen finden Sie unter Bearbeiten einer Verbindung.

# Virtuelle Maschinen

Die Auswahl der Größe einzelner virtueller Maschine beim Erstellen eines Maschinenkatalogs in Studio hängt von den angezeigten Optionen, den Kosten und der Leistung des jeweiligen VM-Instanztyps und der Skalierbarkeit ab.

In Studio werden alle VM-Instanzoptionen angezeigt, die von Microsoft Azure in der jeweiligen Region angeboten werden. Diese Auswahl kann von Citrix nicht geändert werden. Daher sollten Sie mit Ihren Anwendungen und deren CPU-, Arbeitsspeicher- und E/A- Bedarf vertraut sein. Es stehen diverse Optionen zu verschiedenen Preis- und Leistungsstufen zur Auswahl. Einzelheiten zu den Optionen finden Sie in den nachfolgend aufgeführten Microsoft-Artikeln.

- MSDN – Größen virtueller Computer und Cloud-Dienste für Azure: https://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Virtual Machine Pricing: http://azure.microsoft.com/en-us/pricing/details/virtual-machines

**Basic-VMs:** VMs der Klasse "Basic" sind Basisfestplatten. Sie unterliegen primär der von Microsoft unterstützten IOPS-

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Stufe 300. Solche VMs werden für die Arbeitslast von Desktopbetriebssystemen (VDI) und Serverbetriebssystem-RDSHs (Remotedesktop-Sitzungshost) nicht empfohlen.

**Standard-VMs**: VMs der Klasse "Standard" sind in vier Reihen eingeteilt: A, B, DS und G

| Reihe | Anzeige in Studio |
|---|---|
| A | Sehr klein, klein, mittel, groß, sehr groß, A5, A6, A7, A8, A9, A10, A11. Mittel und Groß werden für Tests mit Arbeitslasten der Kategorie Desktopbetriebssystem (VDI) oder Serverbetriebssystem-RDSH empfohlen. |
| D | Standard_D1, D2, D3, D4, D11, D12, D13, D14. Diese VMs bieten SSDs für die temporäre Speicherung. |
| DS | Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Diese VMs bieten einen lokalen SSD-Speicher für alle Datenträger. |
| G | Standard_G1 – G5. Diese VMs sind für High Performance Computing geeignet. |

Stellen Sie beim Provisioning von Maschinen in Azure Storage Premium sicher, dass Sie eine Maschinengröße auswählen, die im Storage Premium-Konto unterstützt wird.

### Kosten- und Leistung von VM-Instanztypen

Die US-Listenpreise der einzelnen VM-Instanztypen pro Stunde sind auf http://azure.microsoft.com/en-us/pricing/details/virtual-machines/ aufgeführt.

Bei der Arbeit mit Cloudumgebungen spielen die tatsächlichen Computing-Anforderungen eine wichtige Rolle. Für Machbarkeitsstudien oder anderen Tests werden gerne Hochleistungs-Instanztypen verwendet. Zur Einsparung von Kosten kann es hingegen verlockend sein, die VMs mit der niedrigsten Leistung zu wählen. Allerdings sollte idealerweise die für die jeweilige Aufgabe am besten geeignete VM verwendet werden. Die VMs der höchsten Leistungsklasse erzielen möglicherweise nicht das gewünschte Ergebnis und werden mit der Zeit sehr teuer – manchmal schon innerhalb einer Woche. Weniger teure VMs einer niedrigen Leistungsklasse sind der jeweiligen Aufgabe u. U. nicht gewachsen.

Tests mit Login VSI bei mittlerer Arbeitslast haben ergeben, dass für Desktopbetriebssysteme (VDI) und Serverbetriebssystem-RDSH Instanzen des Typs "Mittel" (A2) und "Groß" (A3) das beste Preis-/Leistungsverhältnis bieten.

Die Reihen Mittel (A2) und Groß (A3 oder A5) bieten das beste Preis-/Leistungsverhältnis für die Arbeitslastanalyse. Alles darunter wird nicht empfohlen. Leistungsfähigere VM-Reihen bieten ggf. die von Anwendungen und Benutzern geforderte Leistung und Benutzerfreundlichkeit. Es empfiehlt sich jedoch, die drei o. g. Instanztypen als Grundwert anzusetzen, um zu ermitteln, ob die höheren Kosten einer leistungsstärkeren VM einen echten Mehrwert bringen.

### Skalierbarkeit

Die Skalierbarkeit von Katalogen in einer Hostingeinheit unterliegt einigen Schranken. Einige davon, z. B. die Zahl der CPU-Kerne des Azure-Abonnements, können ausgeräumt werden, indem beim Support von Microsoft Azure eine Erhöhung des Standardwerts (20) angefordert wird. Andere, etwa die Zahl der VMs in einem virtuellen Netzwerk pro Abonnement (2048), können nicht geändert werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Derzeit unterstützt Citrix 40 Maschinen pro Katalog.

Zur Erhöhung der Zahl der virtuellen Maschinen in einem Katalog oder Host wenden Sie sich an den Microsoft Azure-Support. Die Standardskalierungslimits von Microsoft Azure verhindern die Überschreitung einer bestimmten Zahl VMs. Diese Limits ändern sich jedoch häufig. Die aktuellen Limits finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/.

Ein Microsoft Azure Virtual Network unterstützt bis zu 2048 VMs.

Microsoft empfiehlt ein Limit von 40 Standarddatenträger-VM-Images pro Clouddienst. Berücksichtigen Sie beim Skalieren die Zahl der Clouddienste, die für die VMs der gesamten Verbindung benötigt werden. Ziehen Sie darüber hinaus die VMs in Betracht, die für gehostete Anwendungen benötigt werden.

Wenden Sie sich an den Support von Microsoft Azure, um in Erfahrung zu bringen, ob die Standardzahl der CPU-Kerne für Ihre Arbeitslasten erhöht werden muss.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Microsoft System Center Configuration Manager-Umgebungen

Jul 08, 2016

Bei Sites, in denen der Zugriff auf Anwendungen und Desktops auf physischen Geräten mit System Center Configuration Manager (Configuration Manager) 2012 verwaltet wird, kann diese Verwendung über die Integrationsoptionen auf XenApp bzw. XenDesktop ausgeweitet werden.

- **Citrix Connector 7.5 für Configuration Manager 2012:** Citrix Connector bildet eine Brücke zwischen Configuration Manager und XenApp bzw. XenDesktop. Mit Citrix Connector können Sie alltägliche Vorgänge in den mit Configuration Manager verwalteten physischen Umgebungen und den mit XenApp bzw. XenDesktop verwalteten virtuellen Umgebungen übergreifend vereinheitlichen. Weitere Informationen zum Connector finden Sie unter Citrix Connector 7.5 für System Center Configuration Manager 2012.
- **Configuration Manager Wake Proxy-Feature:** Unabhängig davon, ob in der Umgebung Citrix Connector verwendet wird, wird für das Wake-On-LAN-Feature für den Remote-PC-Zugriff Configuration Manager benötigt. Weitere Informationen finden Sie weiter unten.
- **XenApp- und XenDesktop-Eigenschaften:** XenApp- und XenDesktop-Eigenschaften ermöglichen die Identifizierung virtueller Citrix Desktops für die Verwaltung durch Configuration Manager. Diese Eigenschaften werden automatisch von Citrix Connector verwendet, sie können aber auch manuell konfiguriert werden, wie im folgenden Abschnitt beschrieben.

Eigenschaften stehen Microsoft System Center Configuration Manager 2012 und 2012 R2 für die Verwaltung virtueller Desktops zur Verfügung.

Boolesche Eigenschaften in Configuration Manager 2012 können als 1 oder 0 statt True oder False angezeigt werden.

Die Eigenschaften stehen in der Klasse Citrix_virtualDesktopInfo im Namespace Root\Citrix\DesktopInformation zur Verfügung. Die Namen der Eigenschaften stammen vom Anbieter für Windows-Verwaltungsinstrumentation (WMI).

| Eigenschaft | Beschreibung |
|---|---|
| AssignmentType | Legt den Wert auf IsAssigned fest. Gültige Werte:<br>• ClientIP<br>• ClientName<br>• Keine<br>• User: legt IsAssigned auf True fest. |
| BrokerSiteName | Site, gibt den gleichen Wert wie HostIdentifier zurück. |
| DesktopCatalogName | Dem Desktop zugewiesener Maschinenkatalog |
| DesktopGroupName | Dem Desktop zugewiesene Bereitstellungsgruppe |
| HostIdentifier | Site, gibt den gleichen Wert wie BrokerSiteName zurück. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Eigenschaft | Beschreibung |
| --- | --- |
| IsAssigned | True = ordnet den Desktop einem Benutzer zu; False = zufälliger Desktop. |
| | |
| IsMasterImage | Ermöglicht Entscheidungen bezüglich der Umgebung. Beispielsweise können Sie Anwendungen auf dem Masterimage und nicht auf den bereitgestellten Maschinen installieren, besonders dann, wenn diese Maschinen auf Bootmaschinen in einem fehlerfreien Zustand sind. Gültige Werte:<br>● True auf einer VM, die als Masterimage verwendet wird (dieser Wert wird während der Installation basierend auf einer Auswahl festgelegt).<br>● Cleared auf einer VM, die von diesem Image bereitgestellt wird. |
| IsVirtualMachine | True für eine virtuelle Maschine, False für eine physische Maschine |
| OSChangesPersist | False, wenn das Betriebssystemimage des Desktops bei jedem Neustart in einen fehlerfreien Zustand versetzt wird, andernfalls True |
| PersistentDataLocation | Der Speicherort, an dem Configuration Manager persistente Daten speichert. Benutzer haben hierauf keinen Zugriff. |
| PersonalvDiskDriveLetter | Bei einem Desktop mit einer persönlichen vDisk ist dies der Laufwerksbuchstabe, den Sie der persönlichen vDisk zuweisen. |
| BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier | Festgelegt, wenn der Desktop sich beim Controller registriert; bei Desktops, die noch nicht vollständig registriert sind, NULL |

Zum Sammeln der Eigenschaften führen Sie eine Hardwareinventur in Configuration Manager durch. Zum Anzeigen der Eigenschaften verwenden Sie den Ressourcen-Explorer von Configuration Manager. In diesen Fällen können die Namen Leerzeichen enthalten oder vom Eigenschaftsnamen etwas abweichen. **BrokerSiteName** kann z. B. als "Broker Site Name" angezeigt werden. Weitere Informationen über die nachfolgend aufgeführten Aufgaben finden Sie unter http://support.citrix.com/article/ctx140905.

- Konfigurieren von Configuration Manager zum Sammeln von Citrix WMI-Eigenschaften vom Citrix VDA
- Erstellen abfragebasierter Gerätesammlungen mit Citrix WMI-Eigenschaften
- Erstellen globaler Bedingungen basierend auf Citrix WMI-Eigenschaften
- Verwenden globaler Bedingungen zum Definieren von Anforderungen für Anwendungsbereitstellungstypen

Sie können in der Microsoft-Klasse CCM_DesktopMachine im Namespace Root\ccm_vdi auch Microsoft-Eigenschaften verwenden. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Zum Konfigurieren des Wake-On-LAN-Features von Remote-PC-Zugriff führen Sie die folgenden Schritte aus, bevor Sie einen VDA auf den Büro-PCs installieren und mit Studio die Remote-PC-Zugriff-Bereitstellung erstellen oder aktualisieren:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Konfigurieren Sie Configuration Manager 2012 im Unternehmen und stellen Sie dann den Configuration Manager-Client auf allen Remote-PC-Zugriff-Maschinen bereit. Warten Sie, bis der geplante SCCM-Bestandszyklus ausgeführt wurde (oder erzingen Sie manuell eine Ausführung). Die Zugriffsanmeldeinformationen, die Sie in Studio zum Konfigurieren der Verbindung mit Configuration Manager angeben, müssen Sammlungen im Geltungsbereich und die Rolle "Remotetoolsverantwortlicher" umfassen.
- Für die Unterstützung von Intel Active Management Technology (AMT) gilt Folgendes:
  - Die unterstützte Mindestversion auf dem PC ist AMT 3.2.1.
  - Stellen Sie den PC für die Verwendung von AMT mit Zertifikaten und zugehörigen Provisioningvorgängen bereit.
- Für die Unterstützung von Configuration Manager Wake-Proxy bzw. von Magic Packet:
  - Konfigurieren Sie Wake-On-LAN in den BIOS-Einstellungen aller PCs.
  - Zur Unterstützung von Configuration Manager Wake Proxy aktivieren Sie die entsprechende Option in Configuration Manager. Stellen Sie für jedes Subnetz des Unternehmens mit PCs, auf denen das Wake-On-LAN-Feature von Remote-PC-Zugriff verwendet wird, sicher, dass mindestens drei Maschinen als Sentinelmaschinen fungieren können.
  - Zur Unterstützung von Magic Packet konfigurieren Sie Netzwerkrouter und Firewalls so, dass Magic Packets entweder per subnetzgesteuertem Broadcast oder Unicast gesendet werden können.

Nach der Installation des VDAs auf Büro-PCs aktivieren oder deaktivieren Sie die Energieverwaltung beim Erstellen der Remote-PC-Zugriff-Bereitstellung in Studio.

- Wenn Sie die Energieverwaltung aktivieren, geben Sie Verbindungsdetails an, d. h. Adresse und Anmeldeinformationen von Configuration Manager sowie einen Namen.
- Wenn Sie die Energieverwaltung nicht aktivieren, können Sie eine Energieverwaltungsverbindung (Configuration Manager) später hinzufügen und dann einen Remote-PC-Zugriff-Maschinenkatalog zur Aktivierung der Energieverwaltung bearbeiten und die neue Energieverwaltungsverbindung angeben.

Sie können eine Energieverwaltungsverbindung bearbeiten, um die Verwendung von Configuration Manager Wake Proxy und Magic Packets zu konfigurieren und die Paketübertragungsmethode zu ändern.

Weitere Informationen finden Sie im Artikel Remote-PC-Zugriff.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Nutanix-Virtualisierungsumgebungen

Aug 17, 2016

Folgen Sie diesen Anleitungen, wenn Sie mit Nutanix Acropolis virtuelle Maschinen in Ihrer XenApp- oder XenDesktop-Bereitstellung bereitstellen. Der Setupvorgang umfasst die folgenden Aufgaben:

- Installieren und Registrieren des Nutanix-Plug-Ins in der XenApp- oder XenDesktop-Umgebung.
- Erstellen einer Verbindung mit dem Nutanix Acropolis-Hypervisor.
- Erstellen eines Maschinenkatalogs mit dem Snapshot eines Masterimages, das auf dem Nutanix-Hypervisor erstellt wurde.

Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In, das vom Nutanix Support Portal heruntergeladen werden kann: https://portal.nutanix.com.

# Installieren und Registrieren des Nutanix-Plug-Ins

Nach der Installation der XenApp- oder XenDesktop-Komponenten führen Sie die folgenden Schritte aus, um das Nutanix-Plug-In auf den Delivery Controllern zu installieren und zu registrieren. Sie können dann mit Studio eine Verbindung mit dem Nutanix-Hypervisor erstellen und zudem einen Maschinenkatalog erstellen, der einen in der Nutanix-Umgebung erstellten Snapshot von einem Masterimage verwendet.

1. Beziehen Sie das Nutanix-Plug-In von Nutanix und installieren Sie es auf den Delivery Controllern.
2. Stellen Sie sicher, dass ein Nutanix Acropolis-Ordner mit folgendem Pfad erstellt wurde: C:\Programme\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Führen Sie Folgendes aus: **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugin.exe –PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"**.
4. Starten Sie den Citrix Hostdienst, Citrix Brokerdienst und Citrix Maschinenerstellungsdienste neu.
5. Führen Sie die folgenden PowerShell-Cmdlets aus, um sicherzustellen, dass das Nutanix Acropolis-Plug-In registriert wurde:

```
Add-PSSnapin Citrix*
Get-HypHypervisorPlugin
```

# Erstellen einer Verbindung mit Nutanix

Vollständige Informationen zu allen Seiten in den Assistenten zum Erstellen einer Verbindung finden Sie in den Artikeln Erstellen einer Site und Verbindungen und Ressourcen.

Wählen Sie im Assistenten zum Einrichten einer Site oder zum Hinzufügen einer Verbindung und Ressourcen auf der Seite **Verbindung** den Verbindungstyp **Nutanix**. Geben Sie dann die Hypervisoradresse und Anmeldeinformationen sowie einen Namen für die Verbindung ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit.

# Erstellen eines Maschinenkatalogs mit einem Nutanix-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Snapshot

Diese Informationen ergänzen die Anleitungen im Artikel Erstellen von Maschinenkatalogen. Es werden nur die Felder beschrieben, die für Nutanix gelten.

Der von Ihnen ausgewählte Snapshot wird als Vorlage zum Erstellen der VMs im Maschinenkatalog verwendet. Erstellen Sie erst Images und Snapshots in Nutanix, bevor Sie den Maschinenkatalog erstellen.

- Allgemeine Informationen über Masterimages finden Sie im Artikel "Erstellen von Maschinenkatalogen".
- Anleitungen zum Erstellen von Images und Snapshots in Nutanix finden Sie in der Nutanix-Dokumentation, auf die zuvor verwiesen wurde.

Die Seiten **Betriebssystem** und **Maschinenverwaltung** enthalten keine Nutanix-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.

Wählen Sie auf der Seite **Container** (nur für Nutanix) den Container aus, in dem die Datenträger der VMs gespeichert werden.

Wählen Sie auf der Seite **Masterimage** den Snapshot des Images aus.

Geben Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl von Kernen pro vCPU an.

Die Seiten **Netzwerkkarten**, **Computerkonten** und **Zusammenfassung** enthalten keine Nutanix-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren über die grafische Oberfläche

Jul 08, 2016

**Hinweis:** Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Verwenden des Produktinstallationsprogramms
- Verwenden des dedizierten VDA-Installationsprogramms
- Anpassen eines VDA


# Einführung

**Wichtig:** Lesen Sie vor Beginn jeglicher Installation den Artikel Vorbereiten der Installation. Er enthält eine Beschreibung der Installationsprogramme und wichtige Informationen, mit denen Sie sich vor der Installation vertraut machen müssen. Er enthält zudem einen Leitfaden für die Elemente, die Sie im Assistenten festlegen müssen. In diesem Abschnitt wird beschrieben, wie Sie die grafische Oberfläche in einem Produktinstallationsprogramm starten.

Die grafische Oberfläche ermöglicht Folgendes:

- Installieren einer oder mehrerer der Kernkomponenten: Delivery Controller, Citrix Studio, Citrix Director, Lizenzserver und StoreFront.
- Installieren von Virtual Delivery Agent (VDA) auf einem Masterimage bzw. auf einer virtuellen oder physischen Maschine. Sie können auch die Skripts anpassen, die auf dem Medium sind, und sie zum Installieren und Entfernen von VDAs in Active Directory verwenden.
- Anpassen bereits installierter VDAs.
- Installieren eines universellen Druckservers. Der Controller hat bereits die Clientfunktionen des universellen Druckerservers; Sie müssen nur die Serverkomponente auf den Druckservern installieren. Nach der Installation der Komponente folgen Sie den Anweisungen im Artikel zum Konfigurieren von Druckern.
- Aktualisieren von Komponenten; Informationen hierzu finden Sie unter Upgrade einer Bereitstellung.

Das Produktinstallationsprogramm und das dedizierte VDA-Installationsprogramm haben beide eine grafische Benutzeroberfläche.

# Verwenden des Produktinstallationsprogramms

Sie können Kernkomponenten, VDAs und die Komponenten des universellen Druckservers mit dem Produktinstallationsprogramm installieren.

1. Laden Sie das Produktpaket von Citrix herunter. Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen.
2. Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.
3. Melden Sie sich mit einem lokalen Administratorkonto am Server an, auf dem Sie die Komponenten installieren.
4. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Doppelklicken Sie auf **Automatische Auswahl**, wenn das Installationsprogramm nicht automatisch gestartet wird, oder klicken Sie auf das bereitgestellte

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Laufwerk.
5. Wählen Sie aus, ob XenApp oder XenDesktop installiert werden soll.
6. Wählen Sie die Komponente aus, die Sie installieren möchten:

- Wenn Sie ganz zu Beginn der Installation stehen, wählen Sie in der linken Spalte **Delivery Controller**. Im Lauf der Installation mit dem Assistenten können Sie auswählen, welche Komponenten (Delivery Controller, Studio, Director, Lizenzserver und StoreFront) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, installiert werden sollen.
- Wenn Sie bereits einige Komponenten installiert haben und Ihre Bereitstellung erweitern möchten, klicken Sie in der rechten Spalte auf die zu installierende Komponente. Diese Spalte enthält Kernkomponenten und den universellen Druckserver.
- Klicken Sie zum Installieren eines VDA auf den VDA-Eintrag in der mittleren Spalte. Es stehen nur die VDAs zur Verfügung, die für das Betriebssystem, unter dem Sie das Installationsprogramm ausführen, geeignet sind.

Folgen Sie die Anweisungen des Assistenten. Informationen zu den Elementen, die Sie im Assistenten sehen und konfigurieren, finden Sie unter Vorbereiten der Installation. Für die Installation eines VDA ist standardmäßig ein automatischer Neustart nach Installationsabschluss aktiviert; dieser ist erforderlich, bevor der VDA in einer Site verwendet werden kann.

# Verwenden des dedizierten VDA-Installationsprogramms

**Wichtig:** Informationen zu Elementen der Installation mit dem dedizierten VDA-Installationsprogramm, insbesondere zu Neustarts und dem für die Extraktion benötigen Speicherplatz, finden Sie unter Vorbereiten der Installation.

Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen. Für die Installation benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**. Deaktivieren Sie die Benutzerkontensteuerung (UAC).

1. Laden Sie das benötigte Paket von Citrix herunter: **VDAServerSetup.exe** für Serverbetriebssystemmaschinen oder **VDAWorkstationSetup.exe** für Desktopbetriebssystemmaschinen Verwenden Sie für Einzelbenutzer-Einzelserverbereitstellungen (z. B. beim Bereitstellen von Windows Server 2012 für einen Benutzer zur Webentwicklung) das Paket VDAWorkstationSetup.exe. Weitere Informationen finden Sie im Artikel "Server-VDI".
2. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Als Administrator ausführen**.
3. Folgen Sie die Anweisungen des Assistenten. Ein automatischer Neustart nach Installationsabschluss ist standardmäßig aktiviert; dieser ist erforderlich, bevor der VDA in einer Site verwendet werden kann.

# Anpassen eines VDA

Einen installierten VDA können Sie auf folgende Weise anpassen:

1. Klicken Sie in Windows im Dialogfeld zum Hinzufügen oder Entfernen von Programmen mit der rechten Maustaste auf **Citrix Virtual Delivery Agent <*Version*>** und wählen Sie **Ändern**.
2. Wählen Sie **Virtual Delivery Agent-Einstellungen anpassen**. Wenn das Installationsprogramm startet, können Sie die Controlleradressen ändern sowie den TCP/IP-Port für die Registrierung beim Controller (Standard = 80) festlegen und ob


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Portausnahmen für die Windows-Firewall automatisch geöffnet werden sollen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren über die Befehlszeile

Jul 11, 2016

**Hinweis:** Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Verwenden des Produktinstallationsprogramms
- Verwenden des dedizierten VDA-Installationsprogramms
- Anpassen eines VDAs über die Befehlszeile
- Befehlszeilenoptionen zur Installation der Kernkomponenten
- Befehlszeilenoptionen zur VDA-Installation
- Installieren des universellen Druckservers über die Befehlszeile


# Einführung

**Wichtig:** Lesen Sie vor Beginn jeglicher Installation den Artikel Vorbereiten der Installation. Er enthält eine Beschreibung der Installationsprogramme und wichtige Informationen, mit denen Sie sich vor der Installation vertraut machen müssen. Außerdem werden die Optionen für die einzelnen Befehle erläutert. In diesem Abschnitt wird beschrieben, wie Sie die Befehlszeilenschnittstelle in einem Produktinstallationsprogramm starten.

Mit der Befehlszeilenschnittstelle können Sie folgende Aufgaben erledigen:

- Installieren einer oder mehrerer der Kernkomponenten: Delivery Controller, Citrix Studio, Citrix Director, Lizenzserver und StoreFront.
- Installieren von Virtual Delivery Agent (VDA) auf einem Masterimage bzw. auf einer virtuellen oder physischen Maschine. Sie können auch die Skripts anpassen, die auf dem Medium sind, und sie zum Installieren und Entfernen von VDAs in Active Directory verwenden.
- Anpassen bereits installierter VDAs.
- Installieren eines universellen Druckservers, der Netzwerksitzungsdrucker bereitstellt. Der Controller hat bereits die universelle Druckerserverfunktionalität; Sie müssen nur den universellen Druckserver auf den Druckservern in der Umgebung installieren.
- Aktualisieren von Komponenten; Informationen hierzu finden Sie unter Upgrade einer Bereitstellung.

Mit den Optionen /remove oder /removeall können Sie zudem zuvor installierte Komponenten aus dieser Version entfernen. Weitere Informationen finden Sie im Artikel Entfernen von Komponenten.

Sie müssen der ursprüngliche Administrator sein oder **Als Administrator ausführen** verwenden, um den Fortschritt der Befehlsausführung und die Rückgabewerte anzuzeigen. Weitere Informationen finden Sie in der Microsoft-Befehlsdokumentation.

Das Produktinstallationsprogramm und das dedizierte VDA-Installationsprogramm haben beide eine Befehlszeilenschnittstelle.

Wenn Sie VDA-Maschinen mit den Beispielskripts installieren, aktualisieren oder aus Active Directory entfernen, können Sie die unten aufgeführten VDA-Konfigurationsoptionen im VDA-Abschnitt angeben. Weitere Informationen zu den Beispielskripts finden Sie im Artikel Installieren von VDAs mit Skripts.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# Verwenden des Produktinstallationsprogramms

Sie können Kernkomponenten und VDAs mit dem Produktinstallationsprogramm installieren.

- Laden Sie das Produktpaket von Citrix herunter. Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen.
- Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.
- Melden Sie sich mit einem lokalen Administratorkonto am Server an, auf dem Sie die Komponenten installieren.
- Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit.
- Führen Sie im Setupverzeichnis \x64\XenDesktop auf dem Medium folgenden Befehl aus:

  **XenDesktopServerSetup.exe** zum Installieren der Kernkomponenten. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur Installation der Kernkomponenten aufgeführten Optionen.

  **XenDesktopVDASetup.exe** zum Installieren eines VDAs. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen.

Beispiel 1: Mit dem folgenden Befehl werden ein XenDesktop-Controller, Studio, die Citrix Lizenzierung und SQL Server Express auf dem Server installiert. Für die Komponentenkommunikation erforderliche Ports werden automatisch geöffnet.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver
/configure_firewall
```

Beispiel 2: Mit dem folgenden Befehl werden ein XenApp-Controller, Studio und SQL Server Express auf dem Server installiert. Für die Komponentenkommunikation erforderliche Ports werden automatisch geöffnet.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components  controller,desktopstudio
/configure_firewall
```

Beispiel 1: Mit dem folgenden Befehl wird ein VDA für Windows-Desktopbetriebssysteme und Citrix Receiver am Standardspeicherort auf einer VM installiert. VDA wird als Masterimage verwendet. Der VDA registriert sich anfänglich am Controller auf dem "Contr-Main" genannten Server in der Domäne "mydomain" und verwendet Personal vDisks, das Optimierungsfeature und die Windows-Remoteunterstützung.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components  vda,plugins /controllers "Contr-
Main.mydomain.local" /enable_hdx_ports /optimize  /masterimage /baseimage /enable_remote_assistance
```

Beispiel 2: Mit dem folgenden Befehl wird ein VDA für Windows-Desktopbetriebssysteme und Citrix Receiver am Standardspeicherort eines Büro-PCs installiert, der mit Remote-PC-Zugriff verwendet wird. Nach der Installation von VDA wird die Maschine nicht neu gestartet. Ein Neustart ist jedoch erforderlich, bevor VDA verwendet werden kann. Der VDA registriert sich anfänglich am Controller auf dem "Contr-East" genannten Server in der Domäne "mydomain" und verwendet UDP für Audiopakete. HDX-Ports werden geöffnet, wenn der Windows-Firewalldienst erkannt wird.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet  /components vda,plugins /controllers "Contr-
East.mydomain.local" /enable_hdx_ports  /enable_real_time_transport /noreboot
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwenden des dedizierten VDA-Installationsprogramms

**Wichtig:** Informationen zu Elementen der Installation mit dem dedizierten VDA-Installationsprogramm, insbesondere zu Neustarts und dem für die Extraktion benötigen Speicherplatz, finden Sie unter Vorbereiten der Installation.

Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen. Für die Installation benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**.

1. Laden Sie das benötigte Paket von Citrix herunter: **VDAServerSetup.exe** für Serverbetriebssystemmaschinen oder **VDAWorkstationSetup.exe** für Desktopbetriebssystemmaschinen Verwenden Sie für Einzelbenutzer-Einzelserverbereitstellungen (z. B. beim Bereitstellen von Windows Server 2012 für einen Benutzer zur Webentwicklung) das Paket VDAWorkstationSetup.exe. Weitere Informationen finden Sie im Artikel Server-VDI.
2. Extrahieren Sie entweder zunächst die Dateien aus dem Paket und führen Sie dann den Installationsbefehl aus oder führen Sie das Paket direkt aus.

   Verwenden Sie zum Extrahieren der Dateien vor der Installation **/extract** mit dem absoluten Pfad, z. B. .\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia. Führen Sie dann mit einem separaten Befehl **XenDesktopVdaSetup.exe** in dem Verzeichnis mit dem extrahierten Inhalt aus (im Beispiel oben wäre dies CitrixVDAInstallMedia). Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen.

   Zu Ausführen des heruntergeladenen Pakets führen Sie dessen Namen **VDAServerSetup.exe** oder **VDAWorkstationSetup.exe** aus. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen. Hinweis für Personen, die mit dem Produktinstallationsprogramm vertraut sind: Die Ausführung des heruntergeladenen eigenständigen Pakets ist mit dem Befehl "XenDesktopVdaSetup.exe" mit Ausnahme des Namens identisch.

Der nachfolgende Installationsbefehl wird oft für Remote-PC-Zugriff verwendet. Mit ihm wird ein VDA auf einem physischen Computer ohne Citrix Receiver oder Citrix Profile Manager installiert. Nach der Installation des VDA wird die Maschine nicht automatisch neu gestartet. Ein Neustart ist jedoch erforderlich, bevor der VDA verwendet werden kann. Zu Beginn wird der VDA auf dem Server 'Contr-East' beim Controller registriert. Wenn der Windows-Firewalldienst erkannt wird, werden Ports geöffnet.

```
VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

> **Hinweis**
>
> Ausschließen von Citrix User Profile Manager aus der Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten "Benutzerdetails" und "Endpunkte" treten Fehler in den Bereichen "Personalisierung" und "Anmeldedauer" auf. Auf den Seiten "Dashboard" und "Trends" werden im Bereich "Durchschnittliche Anmeldedauer" nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anpassen eines VDAs über die Befehlszeile

Nachdem VDA installiert wurde, können Sie einige Einstellungen anpassen. Führen Sie auf dem Produktmedium im Setupverzeichnis \x64\XenDesktop den Befehl **XenDesktopVdaSetup.exe** aus und legen Sie dabei eine oder mehrere der folgenden, im Abschnitt Befehlszeilenoptionen zur VDA-Installation unten beschriebenen Optionen fest:

- /reconfigure: Diese Option ist zum Anpassen von VDA erforderlich
- /h oder /help
- /quiet
- /noreboot
- /controller
- /portnumber port
- /enable_hdx_ports

# Befehlszeilenoptionen zur Installation der Kernkomponenten

In der folgenden Tabelle werden die für den Befehl **XenDesktopServerSetup.exe** verfügbaren Optionen aufgeführt.

| Option | Beschreibung |
|---|---|
| /components component [,component] ... | Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:<br>• CONTROLLER – Controller<br>• DESKTOPSTUDIO – Studio<br>• DESKTOPDIRECTOR – Director<br>• LICENSESERVER – Citrix Lizenzserver<br>• STOREFRONT – StoreFront<br>Wenn diese Option ausgelassen wird, werden alle Komponenten installiert (bzw. entfernt, wenn die Option /remove ebenfalls angegeben ist). |
| /configure_firewall | Öffnet alle Ports in der Windows-Firewall, die für die installierten Komponenten erforderlich sind, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie die Firewall eines Drittanbieters verwenden oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. |
| /help oder/h | Zeigt die Hilfe für Befehle an. |
| /installdir Verzeichnis | Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | Standard: C:\Programme\Citrix |
| /logpath Pfad | Speicherort der Protokolldateien. Der angegebene Ordner muss bereits vorhanden sein. Er wird nicht vom Installationsprogramm erstellt. Standard = "%TEMP%\Citrix\XenDesktop Installer" |
| /no_remote_assistance | (Gilt nur für die Installation von Director.) Deaktiviert das Feature zur Benutzerspiegelung, welches Microsoft-Remoteunterstützung verwendet. |
| /noreboot | Verhindert einen Neustart nach der Installation. (Bei den meisten Kernkomponenten ist ein Neustart in der Standardeinstellung nicht aktiviert). |
| /nosql | Verhindert die Installation von Microsoft SQL Server Express auf dem Server, auf dem Sie den Controller installieren. Wenn diese Option ausgelassen wird, wird SQL Server Express installiert. |
| /quiet oder /passive | Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet. |
| /remove | Entfernt die mit /components angegebenen Kernkomponenten. |
| /removeall | Entfernt alle installierten Kernkomponenten. |
| /tempdir Verzeichnis | Das Verzeichnis, das die temporären Dateien während der Installation enthält. Standard = C:\Windows\Temp. |
| /xenapp | Installiert XenApp. Wenn diese Option ausgelassen wird, wird XenDesktop installiert. |

# Befehlszeilenoptionen zur VDA-Installation

In der folgenden Tabelle werden die für den Befehl **XenDesktopVDASetup.exe** verfügbaren Optionen aufgeführt.

Bei der Installation von VDA für die Verwendung mit Remote-PC-Zugriff geben Sie nur Optionen ein, die auf physischen Maschinen (nicht VMs oder Masterimages) gültig und für VDAs für Windows-Desktopbetriebssysteme relevant sind.

Wenn nicht anders angegeben, gelten die Optionen für physische und virtuelle Maschinen sowie für VDAs für Windows-Desktopbetriebssysteme und VDAs für Windows-Serverbetriebssysteme.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Important

Verwenden Sie in XenApp und XenDesktop 7.9 die Befehlszeile nur für **Remote-PC-Zugriff**-Bereitstellungen und ändern Sie nicht die Syntax für /components und /remotepc. Beispiel:

> VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE "AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet

Wenn /remotepc vor /components steht, wird die Option /remotepc ignoriert.

| Option | Beschreibung |
|---|---|
| /baseimage | (Gilt nur für die Installation von VDA für Windows-Desktopbetriebssysteme auf einer VM.) Ermöglicht das Verwenden von persönlichen vDisks mit einem Masterimage. Weitere Informationen finden Sie im Artikel Personal vDisks. |
| /components component[,component] | Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:<br>• VDA: Installation von VDA<br>• PLUGINS: Installation von Citrix Receiver für Windows (CitrixReceiver.exe)<br>Verwenden Sie zum Beispiel zum Installieren des VDAs ohne Citrix Receiver "/components vda".<br>Wenn diese Option ausgelassen wird, werden alle Komponenten installiert. |
| /controllers "controller [controller] [...]" | Durch Leerzeichen getrennte, vollqualifizierte Domänennamen (FQDNs) der Controller, mit denen VDA kommunizieren kann; von Anführungszeichen umschlossen. Geben Sie nicht beide Optionen, /site_guid und /controllers, an. |
| /enable_framehawk_port | Öffnet die von Framehawk verwendeten UDP-Ports. Standard = false |
| /enable_hdx_3d_pro | Installiert VDA für HDX 3D Pro. Weitere Informationen finden Sie im Artikel HDX 3D Pro. |
| /enable_hdx_ports | Öffnet die erforderlichen Ports für den Controller und die angegebenen Features (Windows-Remoteunterstützung, Echtzeitübertragung und Optimieren) in der Windows Firewall, wenn der Windows-Firewalldienst erkannt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. |
| /enable_real_time_transport | Aktiviert oder deaktiviert die Verwendung von UDP für Audiopakete (Echtzeittransport für Audio). Das Aktivieren dieses Features kann die Audioleistung verbessern. Verwenden Sie die Option "/enable_hdx_ports", wenn Sie möchten, dass die UDP-Ports automatisch bei Erkennung des Windows-Firewalldiensts geöffnet werden. |
| /enable_remote_assistance | Aktiviert das Spiegelungsfeature in der Microsoft-Remoteunterstützung für die Verwendung mit Director. Wenn Sie diese Option angeben, wird der TCP-Port 3389 durch Windows in der Firewall geöffnet, selbst wenn die Option /enable_hdx_ports ausgelassen wird. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| /exclude "component"[,"component"] | Verhindert die Installation der in Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Beispiel: Installieren oder Aktualisieren eines VDAs auf einem nicht mit Maschinenerstellungsdiensten verwalteten Image erfordert keine Personal vDisk- oder Maschinenidentitätsdienstkomponenten. Gültige Werte:<br><br>• Personal vDisk<br>• Maschinenidentitätsdienst<br>• Citrix User Profile Manager<br><br>Das Ausschließen von Citrix User Profile Manager aus der VDA-Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten "Benutzerdetails" und "Endpunkte" treten Fehler in den Bereichen "Personalisierung" und "Anmeldedauer" auf. Auf den Seiten "Dashboard" und "Trends" werden im Bereich "Durchschnittliche Anmeldedauer" nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist. |
| /h oder /help | Zeigt die Hilfe für Befehle an. |
| /installdir Verzeichnis | Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\Citrix |
| /logpath Pfad | Speicherort der Protokolldateien. Der angegebene Ordner muss bereits vorhanden sein. Er wird nicht vom Installationsprogramm erstellt. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar.) Standard = "%TEMP%\Citrix\XenDesktop Installer" |
| /masterimage | (Gilt nur für die Installation von VDA auf einer VM.) Richtet den VDA als Masterimage ein. |
| /no_appv | Verhindert die Installation der Citrix App-V Komponenten. Weitere Informationen finden Sie im Artikel App-V. |
| /nocitrixwddm | (Gilt nur für Windows 7-Maschinen, die keine WDDM-Treiber enthalten.) Deaktiviert die Installation des Citrix WDDM-Treibers. |
| /nodesktopexperience | (Gilt nur für die Installation von VDA für Windows-Serverbetriebssysteme.) Verhindert das Aktivieren von Enhanced Desktop Experience. Dieses Feature wird auch über die Citrix Richtlinieneinstellung "Enhanced Desktop Experience" gesteuert. |
| /noreboot | Verhindert einen Neustart nach der Installation. VDA steht erst nach einem Neustart vollständig zur Verfügung. |
| /optimize | Aktiviert die Optimierung für VDAs, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Geben Sie diese Option für Remote-PC-Zugriff nicht an. Weitere Informationen zum Optimierungstool finden Sie unter CTX125874. |
| /portnumber port | (Gilt nur, wenn die Option /reconfig angegeben wurde.) Portnummer für die Kommunikation zwischen VDA und dem Controller. Der zuvor konfigurierte Port wird deaktiviert, es sei denn, es handelt sich um Port 80. |
| /quiet oder /passive | Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installations- und Konfigurationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet. |
| /reconfig | Passt die zuvor konfigurierten VDA-Einstellungen an, wenn der Befehl mit den Optionen /portnumber, /Controller |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | oder /enable_hdx_ports verwendet wird. Wenn Sie diese Option ohne die Option /quiet angeben, wird die grafische Oberfläche zum Anpassen von VDA gestartet. |
| /remotepc | Verhindert die Installation der folgenden Komponenten auf einem Desktopbetriebssystem (Workstation):<br>• App V-Komponente: Citrix Personalisierung für App-V - VDA<br>• UpmComponent: Citrix User Profile Manager<br>• UpmVdaPlugin-Komponente: Citrix User Profile Manager WMI-Plug-In<br>• Mps Component: Maschinenidentitätsdienst<br>• VDisk-Komponente: Personal vDisk<br>Wenn diese Komponenten während eines Upgrades installiert werden, werden sie vom Installationsprogramm erkannt und aktualisiert. |
| /remove | Entfernt die mit /components angegebenen Komponenten. |
| /removeall | Entfernt alle installierten VDA-Komponenten. |
| /servervdi | Installiert einen VDA für Windows-Desktopbetriebssysteme auf einem unterstützten Windows Server. Lassen Sie diese Option aus, wenn Sie einen VDA für Windows-Serverbetriebssysteme auf einem Windows Server installieren. Lesen Sie vor dem Verwenden dieser Option den Artikel Server-VDI. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar.) |
| /site_guid guid | GUID (Globally Unique Identifier) der Website Active Directory Organisationseinheit (OU). Dabei wird ein virtueller Desktop einer Site zugeordnet, wenn Active Directory für die Discovery verwendet wird (das Feature für automatische Updates ist die empfohlene und Discovery-Standardmethode). Die Site-GUID ist eine Site-Eigenschaft, die in Studio angezeigt wird. Geben Sie nicht beide Optionen, /site_guid und /controllers, an. |
| /tempdir Verzeichnis | Das Verzeichnis für die temporären Dateien während der Installation. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar.) Standard = C:\Windows\Temp. |
| /virtualmachine | (Gilt nur für die Installation von VDA auf einer VM.) Überschreibt das Erkennen einer physischen Maschine durch den Installer. Dabei werden BIOS-Informationen an die VMs weitergegeben, sodass sie als physische Maschinen erscheinen. |
| /xa_server_location url | URL des Servers für Windows Serveranwendungen. |

# Installieren des universellen Druckservers über die Befehlszeile

**Hinweis:** Wenn Sie die UpsServer-Komponente auf einem Server mit der 32-Bit-Version von Windows 2008 installieren, führen Sie die unter Vorbereiten der Installation des universellen Druckservers unter Windows 2008 Server (32-Bit) beschriebenen Schritte aus.

Führen Sie einen der folgenden Befehle auf jedem Druckserver aus:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Unterstütztes 32-Bit-Betriebssystem: Führen Sie die Datei **UpsServer_x86.msi** aus, die sich auf dem Citrix Installationsmedium im Verzeichnis \x86\Universal Print Server\ befindet.
- Unterstütztes 64-Bit-Betriebssystem: Führen Sie die Datei **UpsServer_x64.msi** aus, die sich auf dem Citrix Installationsmedium im Verzeichnis \x64\Universal Print Server\ befindet.

Nach der Installation des universellen Druckservers auf den Druckservern konfigurieren Sie diesen anhand der Anweisungen im Artikel Bereitstellen von Druckern.

Zum Bereitstellen von UpsServer_x86.msi auf einer Windows 2008-32-Bit-Maschine müssen Sie die Mindestversion für Windows Installer für cdf_x86.msi und UpsServer_x86.msi mit Visual Basic-Skripts oder einem Tool wie Orca anpassen.

1. Kopieren Sie die 32-Bit-Version des CDF- und des UPS-Installationspakets (**cdf_x86.msi** und **UpsServer_x86.msi**) in einen temporären Ordner.
2. Installieren Sie das WiSumInf.vbs-Skript oder Orca. Beides ist in dem Paket Windows SDK Components for Windows Installer Developers enthalten. Informationen zu dem Skript finden Sie in dem MSDN-Artikel Manage Summary Information.
3. Ändern Sie die Mindestversion für Windows Installer mit einer der folgenden Methoden:

   WiSumInf.vbs-Skript: Kopieren Sie die Datei WiSumInf.vbs in denselben temporären Ordner wie die beiden Citrix MSI-Pakete. Führen Sie dann das Skript für jedes Pakets mit den Parametern **WiSumInf.vbs cdf_x86.msi Pages=405** und **WiSumInf.vbs UpsServer_x86.msi Pages=405** aus.

   Orca: Öffnen Sie jeweils das Paket cdf_x86.msi und UpsServer_x86.msi, wählen Sie im Menü "View" die Option "Summary Information" aus und ändern Sie den Wert im Textfeld **Schema** in **405**.

Nach Abschluss des oben beschriebenen Verfahrens installieren Sie den universellen Druckserver auf dem Druckserver.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren von VDAs mit Skripts

Jul 08, 2016

**Hinweis:** Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Das Installationsmedium enthält Beispielskripts, um Virtual Delivery Agents (VDAs) für Gruppen von Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch auf einzelne Maschinen anwenden und sie zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services verwendet werden.

Erforderliche Zugriffsberechtigungen:

- Für die Skripts ist Lesezugriff für "Jeder" auf der Netzwerkfreigabe erforderlich, auf der der VDA-Installationsbefehl ist. Der Installationsbefehl ist beim vollständigen Produkt-ISO-Image "XenDesktopVdaSetup.exe" und beim eigenständigen Installationsprogramm "VDAWorkstationSetup.exe" bzw. "VDAServerSetup.exe".
- Die Protokolldetails werden auf jeder lokalen Maschine gespeichert. Sollen die Ergebnisse auch zentral zur Überprüfung und Analyse protokolliert werden, benötigen die Skripts Lese- und Schreibzugriff auf der Netzwerkfreigabe für "Jeder".

Um die Ergebnisse der Skriptausführung zu überprüfen, müssen Sie die zentrale Protokollfreigabe untersuchen. Erfasst werden das Skriptprotokoll, das Installationsprogrammprotokoll und die MSI-Installationsprotokolle. Jeder Installations- oder Deinstallationsvorgang wird in einem Ordner mit Zeitstempel aufgezeichnet. Am Präfix "PASS" oder "FAIL" im Ordnertitel ist ersichtlich, ob der Vorgang erfolgreich war oder nicht. Sie können herkömmliche Verzeichnissuchprogramme verwenden, um schnell eine fehlerhafte Installation oder Deinstallation im zentralen Protokoll zu finden, statt lokal auf den Zielmaschinen zu suchen.

**Wichtig:** Vor Beginn einer Installation führen Sie die im Artikel Vorbereiten der Installation beschriebenen Schritte durch.

# Installieren oder Aktualisieren von VDAs mit dem Skript

1. Besorgen Sie sich das Beispielskript InstallVDA.bat aus \Support\AdDeploy\ auf dem Installationsmedium. Citrix empfiehlt, dass Sie ein Backup der ursprünglichen Skriptdatei anlegen, bevor Sie sie ändern.
2. Bearbeiten Sie das Skript:
   - Geben Sie die Version des zu installierenden VDA an: SET DESIREDVERSION. Beispielsweise kann die Version 7 als 7.0 angegeben werden. Der vollständige Wert befindet sich auf dem Installationsmedium in der Datei ProductVersion.txt (z. B. 7.0.0.3018); eine vollständige Übereinstimmung ist jedoch nicht erforderlich.
   - Geben Sie die Netzwerkfreigabe an, von der das Installationsprogramm aufgerufen wird Verweisen Sie auf den Stamm des Layouts (der höchste Punkt der Struktur): die geeignete Version des Installationsprogramms (32 Bit oder 64 Bit) wird automatisch aufgerufen, wenn das Skript ausgeführt wird. Beispiel: SET DEPLOYSHARE=\\fileserver1\share1.
   - Geben Sie optional einen Netzwerkfreigabeort zum Speichern der zentralen Protokolle an. Beispiel: SET LOGSHARE=\\fileserver1\log1.
   - Geben Sie die VDA-Konfigurationsoptionen wie im Artikel Installieren über die Befehlszeile beschrieben ein. Die Optionen /quiet und /noreboot sind standardmäßig im Skript enthalten und sind erforderlich: SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

3. Weisen Sie mit den Startskripts für Gruppenrichtlinien das Skript der Organisationseinheit in Active Directory zu, in der die Maschinen sind. Diese Organisationseinheit sollte nur Maschinen enthalten, auf denen Sie VDA installieren möchten. Wenn die Maschinen in der Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt und VDA auf jeder Maschine installiert, deren Betriebssystem unterstützt wird.

# Entfernen von VDAs mit dem Skript

1. Besorgen Sie sich das Beispielskript UninstallVDA.bat aus \Support\AdDeploy\ auf dem Installationsmedium. Citrix empfiehlt, dass Sie ein Backup der ursprünglichen Skriptdatei anlegen, bevor Sie sie ändern.
2. Bearbeiten Sie das Skript.
   - Geben Sie die Version des zu entfernenden VDA an: SET CHECK_VDA_VERSION. Beispielsweise kann die Version 7 als 7.0 angegeben werden. Der vollständige Wert befindet sich auf dem Installationsmedium in der Datei ProductVersion.txt (z. B. 7.0.0.3018); eine vollständige Übereinstimmung ist jedoch nicht erforderlich.
   - Geben Sie optional einen Netzwerkfreigabeort zum Speichern der zentralen Protokolle an.
3. Weisen Sie mit den Startskripts für Gruppenrichtlinien das Skript der Organisationseinheit in Active Directory zu, in der die Maschinen sind. Diese Organisationseinheit sollte nur Maschinen enthalten, von denen Sie VDA entfernen möchten. Wenn die Maschinen in der Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt und VDA auf jeder Maschine entfernt.

# Problembehandlung

Das Skript generiert interne Protokolldateien, die den Skriptausführungsverlauf beschreiben. Das Skript kopiert das Protokoll Kickoff_VDA_Startup_Skript innerhalb von Sekunden nachdem die Bereitstellung auf der Maschine gestartet wurde in die zentrale Protokollfreigabe, sodass Sie den Gesamtvorgang überprüfen können. Wenn dieses Protokoll nicht wie vorgesehen in die Protokollfreigabe kopiert wird, können Sie zur weiteren Fehlerbehebung die lokale Maschine untersuchen, denn durch das Skript werden zwei Debugging-Protokolldateien im Ordner %temp% auf jeder Maschine gespeichert:

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

Überprüfen Sie den Inhalt dieser Protokolle, um Folgendes für das Skript sicherzustellen:

- Es wird wie erwartet ausgeführt.
- Das Zielbetriebssystem wird korrekt erkannt.
- Der Verweis auf ROOT von DEPLOYSHARE ist korrekt konfiguriert (enthält die Datei "AutoSelect.exe").
- Die Authentifizierung bei den Freigaben DEPLOYSHARE und LOG ist möglich.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren von VDAs unter Red Hat Linux

Jul 08, 2016

Sie können virtuelle Linux-Desktops auf der Basis einer Red Hat/CentOS-Distribution erstellen. Bereiten Sie die Linux-VMs vor, installieren Sie die neue Software darauf, konfigurieren Sie den Delivery Controller und stellen Sie die Desktops den Benutzern mit Studio zur Verfügung.

Weitere Informationen finden Sie in diesem Artikel.

> **Hinweis**
>
> Die in diesem Dokument verwendeten Linux-Shellbefehle wurden für die GNU Bash-Shell verifiziert.

Der Artikel enthält die folgenden Abschnitte:


- Systemanforderungen
- Konfigurieren von Delivery Controllern
- Vorbereiten von Linux-Maschinen für die VDA-Installation
- Konfigurieren eines Linux-Maschinenkatalogs und einer Bereitstellungsgruppe
- Installieren der Linux VDA-Software
- Ausführen der VDA-Software
- Deinstallieren der Linux VDA-Software
- Problembehandlung
- Bekannte Probleme
- Glossar


# Systemanforderungen

Die folgenden Linux-Distributionen werden vom Linux Virtual Desktop unterstützt:

- SUSE Linux Enterprise:
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CentOS 7.2

> **Hinweis**
>
> In allen Fällen wird die Prozessorarchitektur x86-64 unterstützt.

> **Tipp**
>
> CentOS Linux wird ab Version 1.3 unterstützt. Die Installationsinformationen in diesem Artikel gelten auch für CentOS.

Die folgenden Versionen von XenDesktop werden vom Linux VDA unterstützt:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Die Konfiguration von Linux VDAs ist etwas anders als die von Windows VDAs. Alle Delivery Controller-Farmen können jedoch Windows- und Linux-Desktops vermitteln.

> **Hinweis**
>
> Der Linux VDA ist nicht mit XenDesktop 7.0 oder früheren Versionen kompatibel.

Die folgenden Versionen von Citrix Receiver werden unterstützt:

- Citrix Receiver für Windows Version 4.4 oder höher (dies entspricht v14.4 von wfica32.exe)
- Citrix Receiver für Linux Version 13.3 oder höher
- Citrix Receiver für Mac OSX Version 12.1 oder höher
- Citrix Receiver für Android Version 3.8 oder höher
- Citrix Receiver für iOS Version 6.1.4 oder höher
- Citrix Receiver für Chrome/HTML5 Version 2.0 (nur über Access Gateway)

Die folgenden Hypervisors werden zum Hosten von Linux VDA Gast-VMs unterstützt:

- XenServer
- VMware ESX und ESXi


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft Hyper-V

Bare-Metal-Hosting wird ebenfalls unterstützt.

> **Tipp**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation des Herstellers Ihres Hypervisors.

Die folgenden Active Directory-Integrationspakete oder -produkte werden vom Linux VDA unterstützt:

- Samba Winbind
- Quest Authentication Services v4.1 oder höher
- Centrify DirectControl

> **Tipp**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation des Herstellers Ihres Active Directory-Integrationspakets.

Die folgenden Hypervisors, Linux-Distributionen und NVIDIA GRID™ GPU sind für die Unterstützung von HDX 3D Pro erforderlich.

## Hypervisors

Die folgenden Hypervisors werden unterstützt:

- XenServer
- VMware ESX und ESXi

## Linux-Distributionen

Die folgende Linux-Distribution unterstützt HDX 3D Pro:

- Red Hat Enterprise Linux - Workstation 7.2

## Grafikprozessor

Die folgenden GPUs werden unterstützt:

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

# Konfigurieren von Delivery Controllern

XenDesktop 7.7 oder höher enthält die erforderlichen Änderungen für Linux Virtual Desktop und für frühere Versionen ist


© 1999-2017 Citrix Systems, Inc. All rights reserved.

ein Hotfix oder Updateskript erforderlich. Anleitungen zur Installation und Überprüfung finden Sie in diesem Abschnitt.

Wenden Sie bei XenDesktop 7.6 SP2 das Hotfix Update 2 an, um den Broker für Linux Virtual Desktops zu aktualisieren. Hotfix Update 2 ist hier verfügbar:

- CTX142438: Hotfix Update 2 - für Delivery Controller 7.6 (32 Bit) – Englisch
- CTX142439: Hotfix Update 2 - für Delivery Controller 7.6 (64 Bit) – Englisch

Für frühere XenDesktop-Versionen gibt es das PowerShell-Skript **Update-BrokerServiceConfig.ps1**, mit dem die Konfiguration des Brokerdiensts aktualisiert wird. Es ist im folgenden Paket verfügbar:

- citrix-linuxvda-scripts-1.3.0.zip

Führen Sie die folgenden Schritte auf *jedem* Delivery Controller in der Farm aus:

1. Kopieren Sie das Skript **Update-BrokerServiceConfig.ps1** auf den Delivery Controller.
2. Öffnen Sie als lokaler Administrator eine Windows PowerShell-Konsole.
3. Navigieren Sie zu dem Ordner, der das Skript enthält.
4. Führen Sie das Skript aus:

```
.\Update-BrokerServiceConfig.ps1
```

> **Hinweis**
>
> Standardmäßig verhindert die Konfiguration von PowerShell das Ausführen von PowerShell-Skripts. Wenn das Skript nicht ausgeführt wird, müssen Sie möglicherweise die PowerShell-Ausführungsrichtlinie ändern und das Skript erneut ausführen:
>
> Set-ExecutionPolicy Unrestricted

Das Skript **Update-BrokerServiceConfig.ps1** aktualisiert die Brokerdienstkonfigurationsdatei mit neuen WCF-Endpunkten, die der Linux VDA erfordert, und startet den Brokerdienst neu. Das Skript bestimmt den Speicherort der Brokerdienstkonfigurationsdatei automatisch. Im selben Verzeichnis wird ein Backup der ursprünglichen Konfigurationsdatei mit der Erweiterung **.prelinux** angelegt.

Diese Änderungen haben keine Auswirkungen auf das Brokering von Windows VDAs, die dieselbe Delivery Controller-Farm verwenden. Auf diese Weise kann eine einzige Controller-Farm Sitzungen für Windows und Linux VDAs nahtlos verwalten und vermitteln.

Überprüfen Sie, ob die Zeichenfolge **EndpointLinux** fünf Mal in der Datei angezeigt wird, um zu bestätigen, dass die erforderlichen Konfigurationsänderungen auf einen Delivery Controller angewendet wurden:

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

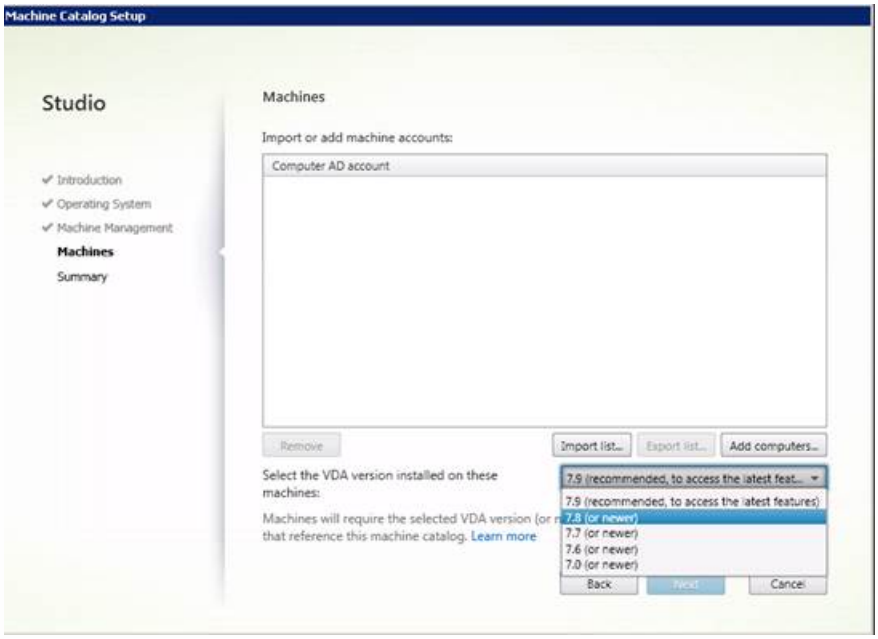
An der Windows-Eingabeaufforderung müssen Sie als lokaler Administrator angemeldet sein:

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

findstr EndpointLinux BrokerService.exe.config

> **Important**
>
> In Version 1.3 ist der Broker-Agent des Linux-VDAs auf XenApp/XenDesktop 7.8 festgelegt. Wird jedoch ein Maschinenkatalog über den Bildschirm zum Einrichten eines Maschinenkatalogs von Studio hinzugefügt, wird der Standardwert automatisch auf Version 7.9 festgelegt. Sie müssen die Version des installierten VDAs explizit auf **7.8 (oder höher)** festlegen. Siehe Abbildung unten.




# Vorbereiten der Linux-Maschine für die VDA-Installation

Citrix empfiehlt, dass Netzwerk zu verbinden und richtig zu konfigurieren, bevor Sie fortfahren.

## Nur für RHEL 6: Festlegen des Hostnamens

Damit der Hostname der Maschine richtig gemeldet wird, ändern Sie die Datei **/etc/sysconfig/network**, sodass sie nur den Hostnamen der Maschine enthält.

HOSTNAME=**hostname**

## Nur für RHEL 7: Festlegen des Hostnamens

Damit der Hostname der Maschine richtig gemeldet wird, ändern Sie die Datei **/etc/hostname**, sodass sie nur den Hostnamen der Maschine enthält.

## Zuweisen einer Loopbackadresse für den Hostnamen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Damit der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine richtig gemeldet werden, ändern Sie die folgende Zeile in der Datei **/etc/hosts**, sodass der FQDN und der Hostname die ersten zwei Einträge sind:

127.0.0.1 **hostname-fqdn hostname** localhost localhost.localdomain localhost4 localhost4.localdomain4

Beispiel:

127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4

Entfernen Sie alle anderen Verweise auf **hostname-fqdn** oder **hostname** aus anderen Einträge in der Datei.

> **Hinweis**
>
> Der Linux VDA unterstützt derzeit keine abgeschnittenen NetBIOS-Namen, daher darf der Hostname nicht länger als 15 Zeichen sein.

> **Tipp**
>
> Verwenden Sie nur Buchstaben (a-z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Hostnamen sollten nicht mit einer Zahl beginnen und nicht mit einem Bindestrich enden.

## Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

hostname

Nur der Hostname der Maschine sollte zurückgegeben werden und nicht der vollqualifizierte Domänenname (FQDN).

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

hostname -f

Der FQDN der Maschine sollte zurückgegeben werden.

## Überprüfen von Namensauflösung und Diensterreichbarkeit

Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den XenDesktop Delivery Controller:

nslookup **domain-controller-fqdn**

ping **domain-controller-fqdn**

nslookup **delivery-controller-fqdn**

ping **delivery-controller-fqdn**

Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den XenDesktop Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem Zeitdienst synchronisiert werden.

RHEL 6.x und frühere Releases verwenden den NTP-Daemon (ntpd) zum Synchronisieren der Uhr, während in einer RHEL 7.x-Standardumgebung der neuere Chrony-Daemon (chronyd) verwendet wird. Die Konfiguration und Betriebsprozesse zwischen den beiden Diensten sind ähnlich.

## Nur für RHEL 6: Konfigurieren des NTP-Diensts

Bearbeiten Sie als Root-Benutzer die Datei **/etc/ntp.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

In einer typischen Bereitstellung sollte die Zeit von den lokalen Domänencontrollern synchronisiert werden und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle anderen Servereinträge, einschließlich Einträge für Loopback-IP-Adressen, Localhost und öffentliche Server wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den NTP-Daemon neu:

sudo /sbin/service ntpd restart

## Nur für RHEL 7: Chrony-Dienst

Bearbeiten Sie als Root-Benutzer die Datei **/etc/chrony.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:

server **peer1-fqdn-or-ip-address** iburst

server **peer2-fqdn-or-ip-address** iburst

In einer typischen Bereitstellung sollte die Zeit von den lokalen Domänencontrollern synchronisiert werden und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle anderen Servereinträge, einschließlich Einträge für Loopback-IP-Adressen, Localhost und öffentliche Server wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den Chrony-Daemon neu:

sudo /sbin/service chronyd restart

In RHEL 6 wird Benutzern aufgrund eines bestimmten Problems nach dem Anmelden ein Popupfenster mit der Aufforderung zur Eingabe des Root-Kennworts angezeigt.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Sie lösen das Problem, indem Sie mit Root-Berechtigungen die Datei **/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla** in einem Texteditor erstellen und den folgenden Inhalt hinzufügen:

```
[No Show Proxy Dialog]

Identity=unix-user:*

Action=org.freedesktop.packagekit.system-network-proxy-configure

ResultAny=no

ResultInactive=no

ResultActive=no
```

> **Tipp**
>
> Weitere Informationen zu diesem Problem finden Sie auf der auf der RedHat Lösungsseite. Der Workaround ist in den Kommentaren beschrieben.

Der Linux VDA ist von OpenJDK abhängig. Die Laufzeitumgebung sollte als Teil der Betriebssysteminstallation installiert worden sein.

## Nur für RHEL 6: OpenJDK 1,7

Bestätigen Sie die richtige Version mit folgendem Befehl:

```
sudo yum info java-1.7.0-openjdk
```

Das OpenJDK-Paket ist möglicherweise eine frühere Version. Aktualisieren Sie ggf. auf die aktuelle Version:

```
sudo yum -y update java-1.7.0-openjdk
```

Legen Sie die Umgebungsvariable **JAVA_HOME** fest, indem Sie der Datei **~/.bashrc** folgende Zeile hinzufügen:

```
export JAVA_HOME=/usr/lib/jvm/java
```

Öffnen Sie eine neue Shell und prüfen Sie die Java-Version:

```
java –version
```

## Nur für RHEL 7,0: OpenJDK 1,8

Bestätigen Sie die richtige Version mit folgendem Befehl:

```
sudo yum info java-1.8.0-openjdk
```

Das OpenJDK-Paket ist möglicherweise eine frühere Version. Aktualisieren Sie ggf. auf die aktuelle Version:

```
sudo yum -y update java-1.8.0-openjdk
```

Legen Sie die Umgebungsvariable **JAVA_HOME** fest, indem Sie der Datei **~/.bashrc** folgende Zeile hinzufügen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
export JAVA_HOME=/usr/lib/jvm/java
```

Öffnen Sie eine neue Shell und prüfen Sie die Java-Version:

```
java –version
```

> **Tipp**
>
> Stellen Sie zum Vermeiden von Problemen sicher, dass die OpenJDK-Version 1.7.0 oder 1.8.0 installiert ist. Entfernen Sie alle anderen auf dem System vorhandenen Java-Versionen.

Der Linux VDA erfordert auf RHEL 6 PostgreSQL 8.4 oder höher und auf RHEL 7 PostgreSQL Versionen 9.2 oder höher.

Installieren Sie die folgenden Pakete:

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

Anschließend ist der folgende Schritt erforderlich, um die Datenbank zu initialisieren und zu gewährleisten, dass der Dienst beim Booten startet. Mit dem Befehl werden unter **/var/lib/pgsql/data** Datenbankdateien erstellt. Der Befehl ist für PostgreSQL 8 und 9 unterschiedlich.

## Nur für RHEL 6: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
```

## Nur für RHEL 7: PostgreSQL 9

```
sudo postgresql-setup initdb
```

## Starten von PostgreSQL

Für beide Versionen von PostgreSQL müssen Sie den Dienst so konfigurieren, dass er beim Booten startet und auch sofort startet:

```
sudo /sbin/chkconfig postgresql on
```

```
sudo /sbin/service postgresql start
```

Überprüfen Sie die Version von PostgreSQL mit folgendem Befehl:

```
psql --version
```

Stellen Sie mit dem **psql**-Befehlszeilenprogramm sicher, dass das Datenverzeichnis festgelegt ist:

```
sudo -u postgres psql -c 'show data_directory'
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Abhängig von der Distribution benötigt der Linux VDA das motif- oder openmotif-Paket.

## Nur für RHEL 6: Öffnen von Motif

```
sudo yum -y install openmotif
```

## Nur für RHEL 7: Motif

```
sudo yum -y install motif
```

Der Linux VDA erfordert Cups- und Foomatic-Filter.

## Nur für RHEL 6: Druckunterstützung

```
sudo yum –y install cups
sudo yum -y install foomatic
```

## Nur für RHEL 7: Druckunterstützung

```
sudo yum –y install cups
sudo yum -y install foomatic-filters
```

Installieren Sie die anderen erforderlichen Pakete:

```
sudo yum -y install redhat-lsb-core
sudo yum -y install ImageMagick
```

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie entsprechend der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

## Festlegen der Zeitsynchronisierung auf Citrix XenServer

Wenn das Zeitsynchronisierungsfeature auf XenServer aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und XenServer gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. Dazu muss die Hostzeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen, auf denen ein paravirtualisierter Linux-Kernel mit installierten XenServer-Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das XenServer- Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
su -
cat /proc/sys/xen/independent_wallclock
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Mögliche Ergebnisse:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.
- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei /proc/sys/xen/indepent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Wenn das Zeitsynchronisierungsfeature aktiviert ist, deaktivieren Sie es, indem Sie "1" in die Datei eingeben:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, bearbeiten Sie die Datei /etc/sysctl.conf und fügen Sie die folgende Zeile hinzu:

```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

```
reboot
```

Nach dem Neustart müssen Sie sicherstellen, dass die Einstellung richtig festgelegt wurde:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Der Wert "1" sollte zurückgegeben werden.

## Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Um sicherzustellen, dass die Betriebssystemzeit korrekt ist, sollten Sie das Feature zusätzlich zu den NTP-Diensten aktivieren.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integrationsdienste**.
3. Stellen Sie sicher, dass **Zeitsynchronisierung** ausgewählt ist.

> ### Hinweis
>
> Diese Methode unterscheidet sich von VMware und XenServer, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.

## Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und der Hypervisor gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. Dazu


© 1999-2017 Citrix Systems, Inc. All rights reserved.

muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Linux-Maschinen können mit verschiedenen Methoden der Active Directory-Domäne hinzugefügt werden, die von XenDesktop für Linux unterstützt wird:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Folgen Sie den Anweisungen unten für die von Ihnen gewählte Methode.

## Samba Winbind

### Installieren oder Aktualisieren der erforderlichen Pakete

Installieren oder aktualisieren Sie die erforderlichen Pakete:

```
sudo yum -y install samba-winbind \
    samba-winbind-clients \
    krb5-workstation \
    authconfig \
    oddjob-mkhomedir
```

### Starten des Winbind-Daemon beim Booten

Der Winbind-Daemon muss zum Starten beim Booten konfiguriert werden:

```
sudo /sbin/chkconfig winbind on
```

### Konfigurieren der Winbind-Authentifizierung

Konfigurieren Sie die Maschine für die Kerberos-Authentifizierung mit Winbind:

```
sudo authconfig \
    --disablecache \
    --disablesssd \
    --disablesssdauth \
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
--enablewinbind \
--enablewinbindauth \
--disablewinbindoffline \
--smbsecurity=ads \
--smbworkgroup=domain \
--smbrealm=REALM \
--krb5realm=REALM \
--krb5kdc=fqdn-of-domain-controller \
--winbindtemplateshell=/bin/bash \
--enablemkhomedir --updateall
```

**REALM** ist der Kerberos-Bereichsname in Großbuchstaben und **domain** ist der kurze NetBIOS-Name der Active Directory-Domäne.

Wenn DNS-basierte Suchvorgänge nach dem KDC-Server und -Bereichsname erforderlich sind, fügen Sie dem oben aufgeführten Befehl die folgenden beiden Optionen hinzu:

```
--enablekrb5kdcdns --enablekrb5realmdns
```

Ignorieren Sie alle Fehler hinsichtlich des Winbind-Dienststarts, die vom Befehl **authconfig** zurückgegeben wurden. Diese sind darauf zurückzuführen, dass authconfig versucht, den Winbind-Dienst zu starten, bevor die Maschine mit einer Domäne verbunden wurde.

Öffnen Sie die Datei **/etc/samba/smb.conf** und fügen Sie im Abschnitt **[Global]** nach dem vom authconfig-Tool erstellten Abschnitt die folgenden Einträge hinzu.

```
kerberos method = secrets and keytab
winbind refresh tickets = true
```

Der Linux VDA benötigt die Systemdatei für die Schlüsseltabelle **/etc/krb5.keytab**, um sich am Delivery Controller zu authentifizieren und zu registrieren. Die Einstellung **kerberos method** zwingt Winbind zum Erstellen der Systemdatei für die Schlüsseltabelle, wenn die Maschine der Domäne beitritt.

### Beitreten zu einer Windows-Domäne

Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo net ads join REALM -U user
```

REALM ist der Kerberos-Bereichsname in Großbuchstaben und user ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

### Konfigurieren von PAM für Winbind

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Standardmäßig wird bei der Konfiguration des Winbind PAM-Moduls **(pam_winbind)** nicht das Zwischenspeichern von Kerberos-Tickets und das Erstellen von Basisverzeichnissen aktiviert. Öffnen Sie die Datei **/etc/security/pam_winbind.conf** und ändern Sie die folgenden Einträge im Abschnitt **[Global]** oder fügen Sie sie hinzu:

```
krb5_auth = yes

krb5_ccache_type = FILE

mkhomedir = yes
```

Entfernen Sie ggf. den Einstellungen vorangehende Semikolons. Diese Änderungen erfordern den Neustart des Winbind-Daemon:

```
sudo /sbin/service winbind restart
```

> **Tipp**
>
> Der Winbind-Daemon wird nur weiterhin ausgeführt, wenn die Maschine zu einer Domäne gehört.

Öffnen Sie die Datei **/etc/krb5.conf** und ändern Sie im Abschnitt [libdefaults] die folgende Einstellung von KEYRING in FILE:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

### Überprüfen der Domänenmitgliedschaft

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben.

Stellen Sie mit dem Samba-Befehl **net ads** sicher, dass die Maschine zu einer Domäne gehört:

```
sudo net ads testjoin
```

Überprüfen Sie zusätzliche Domänen- und Computerobjektinformationen mit folgendem Befehl:

```
sudo net ads info
```

### Überprüfen der Kerberos-Konfiguration

Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Daraufhin sollte die Liste der Schlüssel angezeigt werden, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

```
sudo kinit -k MACHINE\$@REALM
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden und das Dollarzeichen ($) muss durch einen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

umgekehrten Schrägstrich (\) geschützt werden, um die Ersetzung in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

```
sudo klist
```

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

```
sudo net ads status
```

### Überprüfen der Benutzerauthentifizierung

Überprüfen Sie mit dem Tool **wbinfo**, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

```
wbinfo --krb5auth=domain\\username%password
```

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sicherzustellen, dass das Winbind PAM-Modul richtig konfiguriert ist, melden Sie sich lokal mit einem Domänenbenutzerkonto an, mit dem noch nie eine Anmeldung an der Maschine vorgenommen wurde.

```
ssh localhost -l domain\\username
```

```
id -u
```

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung:

```
exit
```

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden.

## Quest Authentication Service

### Konfigurieren von Quest auf dem Domänencontroller

Es wird vorausgesetzt, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über Administratorrechte zum Erstellen von Computerobjekten in Active Directory verfügen.

### Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen

Für alle Domänenbenutzer, die HDX-Sitzungen auf einer Linux VDA-Maschine herstellen, führen Sie folgende Schritte aus:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Öffnen Sie in der Verwaltungskonsole für Active Directory-Benutzer und -Computer die Active Directory-Eigenschaften für das jeweilige Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix Account** aus.
3. Aktivieren Sie das Kontrollkästchen **Unix-enabled**.
4. Legen Sie **Primary GID Number** auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

> **Hinweis**
>
> Mit diesen Anleitungen können Domänenbenutzer für die Anmeldung mit der Konsole, RDP, SSH oder anderen Remotingprotokollen eingerichtet werden.

### Konfigurieren von Quest auf Linux VDA

#### Workaround bei SELinux-Richtlinienerzwingung

In der RHEL-Standardumgebung wird SELinux vollständig erzwungen. Das beeinträchtigt die von Quest verwendeten IPC-Methoden der Unix-Domänensockets und verhindert, dass Domänenbenutzer sich anmelden.

> **Tipp**
>
> Hier finden Sie einige Workarounds.

Am einfachsten ist es, SELinux zu deaktivieren. Bearbeiten Sie als Root-Benutzer die Datei /etc/selinux/config und ändern Sie die SELinux-Einstellung:

```
SELINUX=disabled
```

Diese Änderung erfordert einen Neustart:

```
reboot
```

> **Important**
>
> Seien Sie vorsichtig beim Verwenden dieser Einstellung. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach ihrer Deaktivierung kann selbst für den Root-Benutzer und anderen lokale Benutzer zu einer vollständigen Sperrung führen.

#### Konfigurieren des VAS-Daemon

Die automatische Erneuerung von Kerberos-Tickets muss aktiviert und getrennt sein. Authentifizierung (für Offlineanmeldung) muss deaktiviert sein:

```
sudo /opt/quest/bin/vastool configure vas vasd \
                    auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

allow-disconnected-auth false

Hiermit wird das Verlängerungsintervall auf 9 Stunden (32400 Sekunden) festgelegt. Das ist eine Stunde weniger als die Standardgültigkeitsdauer (10 Stunden) eines Tickets. Bei Systemen mit einer kürzeren Ticketgültigkeitsdauer legen Sie diesen Parameter auf einen niedrigeren Wert fest.

### Konfigurieren von PAM und NSS

Quest erfordert, dass PAM und NSS manuell konfiguriert werden, um Domänenbenutzern die Anmeldung per HDX und anderen Diensten, wie SU, SSH und RDP, zu ermöglichen. Konfigurieren von PAM und NSS:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
```

### Beitreten zu einer Windows-Domäne

Machen Sie die Linux-Maschine mit dem Quest-Befehl "vastool" zu einem Mitglied der Active Directory-Domäne:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der Benutzer ist ein beliebiger Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. Der Domänenname ist der DNS-Name der Domäne, z. B. example.com.

### Überprüfen der Domänenmitgliedschaft

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Quest angemeldete Linux-Maschine zur Domäne gehört:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine zu einer Domäne gehört, wird der Domänenname zurückgegeben. Wenn sie nicht zur Domäne gehört, wird die folgende Fehlermeldung angezeigt:

```
ERROR: No domain could be found.

ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm

default_realm not configured in vas.conf. Computer may not be joined to domain
```

### Überprüfen der Benutzerauthentifizierung

Um sicherzustellen, dass Quest Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto an, mit dem noch nie eine Anmeldung an der Maschine vorgenommen wurde:

```
ssh localhost -l domain\\username

id -u
```

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Stellen Sie sicher, dass die im Tickets Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

```
/opt/quest/bin/vastool klist
```

Beenden Sie die Sitzung:

```
exit
```

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden.

## Centrify DirectControl

**Beitreten zu einer Windows-Domäne**

Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl **adjoin** zu einem Mitglied der Active Directory-Domäne:

```
su –

adjoin -w -V -u user domain-name
```

Der Parameter **user** ist ein Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern von Active Directory-Domänen zu machen. Der Parameter "domain-name" ist der Name der Domäne, der die Linux-Maschine beitritt.

**Überprüfen der Domänenmitgliedschaft**

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

```
su –

adinfo
```

Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

adinfo –diag
```

Testen der Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten:

```
adinfo --test
```

### Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro sind weitere Installationsschritte erforderlich, um die erforderlichen Grafiktreiber auf dem Hypervisor und auf den VDA-Maschinen zu installieren.

Konfigurieren Sie Folgendes:

1. Citrix XenServer
2. VMware ESX

Folgen Sie den Anweisungen für den von Ihnen gewählten Hypervisor.

### Citrix XenServer

In diesem Abschnitt wird die Installation und Konfiguration von NVIDIA GRID-Treibern auf Citrix XenServer detailliert

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

beschrieben.

### VMware ESX

Installieren und konfigurieren Sie die NVIDIA GRID-Treiber für VMware ESX entsprechend den Informationen in diesem Dokument.

### VDA-Maschinen

Führen Sie die folgenden Schritte aus, um die Treiber für die Linux-VM-Gäste zu installieren und zu konfigurieren:

1. Stellen Sie zu Beginn sicher, dass die Linux-VM heruntergefahren ist.
2. Fügen Sie in XenCenter der VM eine GPU im GPU-Passthrough-Modus hinzu.
3. Starten Sie die RHEL-VM.

Zum Vorbereiten der Maschine für die NVIDIA GRID-Treiber sind die folgenden Schritte erforderlich:

```
# yum install gcc

# yum install "kernel-devel-uname-r == $(uname -r)"

# systemctl set-default multi-user.target
```

Wenn Sie diese Schritte ausgeführt haben, folgen Sie den Anleitungen im Red Hat Enterprise Linux-Dokument zum Installieren des NVIDIA GRID-Treibers.

> **Hinweis**
>
> Wählen Sie während der GPU-Treiberinstallation für jede Frage den Standardwert ("no").

> **Important**
>
> Wenn GPU-Passthrough aktiviert wurde, ist über XenCenter kein Zugriff auf die Linux-VM mehr möglich, daher müssen Sie SSH zum Herstellen einer Verbindung verwenden.

Überprüfen Sie, ob der NVIDIA GRID™-Grafiktreiber richtig installiert ist, indem Sie "nvidia-smi" ausführen. Das Ergebnis sollte ungefähr wie folgt aussehen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Legen Sie die richtige Konfiguration für die Karte fest:

etc/X11/ctx-nvidia.sh

Um die hohen Auflösungen und Multimonitorfunktionen nutzen zu können, benötigen Sie eine gültige NVIDIA-Lizenz. Anleitungen zum Anwenden der Lizenz finden Sie in der Produktdokumentation in "GRID Licensing Guide.pdf - DU-07757-001 September 2015".

# Konfigurieren eines Linux-Maschinenkatalogs und einer Bereitstellungsgruppe

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ist der traditionellen Windows VDA-Methode sehr ähnlich. Umfassendere Informationen zu diesen Prozessen finden Sie online in der Citrix Produktdokumentation.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen, durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Windows-Serverbetriebssystem oder Serverbetriebssystem für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Windows-Desktopbetriebssystem oder Desktopbetriebssystem für ein VDI-dediziertes Desktopbereitstellungsmodell.
- Stellen Sie sicher, dass für die Maschinen keine Energieverwaltung festgelegt ist.
- Da PVS und MCS für Linux VDAs nicht unterstützt werden, wählen Sie die Bereitstellungsmethode **Anderer Dienst oder andere Technologie** (vorhandene Images).
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Hinweis**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von Windows-Serverbetriebssystem oder Serverbetriebssystem wird ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von Windows-Desktopbetriebssystem oder Desktopbetriebssystem wird ein Bereitstellungsmodell für XenDesktop Einzelbenutzermaschinen bereitgestellt.

Anleitungen zum Erstellen von Maschinenkatalogen finden Sie in der Citrix Dokumentation unter der jeweiligen Version:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Frühere Versionen von XenDesktop werden nicht unterstützt.

> **Tipp**
>
> Wenn eine Maschine eine Active Directory-Domäne verlässt und ihr dann wieder beitritt, muss die Maschine aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie online in der Citrix Produktdokumentation.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Wählen Sie als Bereitstellungstyp "Desktops" aus. Linux VDA-Maschinen unterstützen keine Bereitstellung von Anwendungen.
- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

Anleitungen zum Erstellen von Bereitstellungsgruppen finden Sie in der Citrix Dokumentation unter der jeweiligen Version:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Frühere Versionen von XenDesktop werden nicht unterstützt.

# Installieren der Linux VDA-Software

Wenn bereits eine ältere Linux VDA-Version als Version 1.0 installiert ist, deinstallieren Sie diese Version, bevor Sie die neue Version installieren.

Halten Sie die Linux VDA-Dienste an:

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```

Deinstallieren Sie das Paket:

```
sudo rpm -e XenDesktopVDA
```

> **Important**
>
> Das Upgrade von der Tech Preview auf Version 1.0, 1.1, 1.2 und 1.3 wird nicht unterstützt.
>
> Für RHEL 6.0, empfiehlt Citrix, dass Sie die Xorg-x11-server-Xorg-Version 1.15 behalten und dieses Paket nicht aktualisieren.

> **Hinweis**
>
> Ab Version 1.3 wurde der Installationspfad geändert. In vorherigen Releases waren die Installationskomponenten unter **/usr/local/**. Der neue Speicherort ist **/opt/Citrix/VDA/**.
>
> Zum Ausführen eines Befehls ist der vollständige Pfad erforderlich. Alternativ können Sie **/opt/Citrix/VDA/sbin** und **/opt/Citrix/VDA/bin** dem Systempfad hinzufügen.

# Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager:

**Für RHEL 6**:

```
sudo rpm -i XenDesktopVDA-1.3.312-1.el6.x86_64.rpm
```

**Für RHEL 7.2**:

```
sudo rpm -i XenDesktopVDA-1.3.312-1.el7.x86_64.rpm
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Sie Version 1.1 oder 1.2 des Linux VDA installiert haben, aktualisieren Sie die Linux VDA-Software mit dem RPM-Paketmanager:

**Für RHEL 6**:

```
sudo rpm -U XenDesktopVDA-1.3.312-1.el6.x86_64.rpm
```

**Für RHEL 7.2**:

```
sudo rpm -U XenDesktopVDA-1.3.312-1.el7.x86_64.rpm
```

> **Important**
>
> Nach dem Upgrade müssen Sie die Linux VDA-Maschine neu starten.

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Wenn Sie das Paket aktualisiert haben, müssen Sie das Skript ctxsetup.sh ausführen, um das Upgrade abzuschließen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Bei Bedarf können Sie dieses Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Das Skript kann manuell mit Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausgeführt werden. Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

## Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

## Automatische Konfiguration

Bei einer automatischen Installation können die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen angegeben werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine weiteren Informationen vom Benutzer und der Installationsvorgang wird per Skript ausgeführt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N: Der Virtual Delivery Agent unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Einstellung ist normalerweise N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns: Der Virtual Delivery Agent erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) von Delivery Controllern
- zur Registrierung mit einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- TX_XDL_VDA_PORT = port-number: Der Virtual Delivery Agent kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist normalerweise Port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N: Der Support für Linux Virtual Desktop-Dienste wird während des Startvorgangs


© 1999-2017 Citrix Systems, Inc. All rights reserved.

gestartet. Die Einstellung ist normalerweise Y.

- CTX_XDL_ADD_FIREWALL_RULES = Y | N: Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Einstellung ist normalerweise Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3: Für den Virtual Delivery Agent müssen Kerberos-Konfigurationseinstellungen von den Delivery Controllern authentifiziert werden. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt. Geben Sie die zu verwendende Active Directory-Integrationsmethode an:
  - 1 – Samba Winbind
  - 2 – Quest-Authentifizierungsdienst
  - 3 – Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N: Linux Virtual Desktop unterstützt HDX 3D Pro, ein Satz Grafikbeschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Für HDX 3D Pro muss eine kompatible NVIDIA Grid-Grafikkarte installiert sein. Wenn HDX 3D Pro aktiviert ist, muss der Virtual Delivery Agent für VDI-Desktopmodus (Einzelsitzungen) konfiguriert werden (d. h. CTX_XDL_VDI_MODE=Y). Dies wird unter SUSE nicht unterstützt. Stellen Sie sicher, dass dieser Wert auf N eingestellt ist.
- CTX_XDL_VDI_MODE: =J | N: Ermöglicht die Konfiguration der Maschine als ein dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Für HDX 3D Pro-Umgebungen muss die Einstellung Y sein. Die Einstellung ist normalerweise N.
- CTX_XDL_SITE_NAME= dns-name: Der Virtual Delivery Agent ermittelt LDAP-Server mit DNS durch die Abfrage von LDAP-Diensteinträgen. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Normalerweise ist nichts angegeben [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers: Der Virtual Delivery Agent fragt standardmäßig DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Diensteinträge ermitteln kann, können Sie eine durch Leerzeichen getrennte Liste mit LDAP-FQDNs mit LDAP-Port angeben (z. B. ad1.mycompany.com:389). Normalerweise ist nichts angegeben [none].
- CTX_XDL_SEARCH_BASE= search-base: Der Virtual Delivery Agent fragt standardmäßig LDAP mit einer Suchbasis ab, die auf den Stamm der Active Directory-Domäne festgelegt ist (z. B. DC=mycompany,DC=com). Zum Verbessern der Suchleistung kann jedoch eine Suchbasis angegeben werden (z. B. OU=VDI,DC=mycompany,DC=com). Normalerweise ist nichts angegeben [none].
- CTX_XDL_START_SERVICE = Y | N: Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Einstellung ist normalerweise Y.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

```
export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Sie müssen die Option -E mit sudo angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile #!/bin/bash enthält.

Alternativ können alle Parameter mit einem einzigen Befehl angegeben werden:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

## Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen u. U. entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

Entfernen von Konfigurationsänderungen:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

## Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in eine Konfigurationsprotokolldatei:

/tmp/xdl.configure.log

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

# Ausführen der VDA-Software

Wenn Sie den Linux VDA mit dem Skript ctxsetup.sh konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start
sudo /sbin/service ctxvda start
```

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx restart
sudo /sbin/service ctxvda start
```

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status
sudo /sbin/service ctxhdx status
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
rpm -q XenDesktopVDA
```

Anzeigen weiterer Details:

```
rpm – qi XenDesktopVDA
```

> **Hinweis**
>
> Beim Deinstallieren der Linux VDA-Software werden die damit verknüpften PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden nicht entfernt.

Dieser Abschnitt bezieht sich nicht auf das Entfernen von abhängigen Paketen einschließlich PostgreSQL.

# Problembehandlung

### Sicherstellen, dass die H.264-Codierung verwendet wird

Linux VDA v1.3 fügt H264 und einen HardwareEncoding-Wert im Registrierungspfad HKLM\Software\Citrix\Ica\Session\\Graphics hinzu, um die Problembehandlung von Grafikproblemen, die beim VDA auftreten, zu unterstützen.

Führen Sie den folgenden Befehl aus, um die H.264-Codierung in einem Linux-VDA vor dem Start einer Sitzung anzukündigen:

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"AdvertiseH264" -d "0x00000001" --force
```

Starten Sie die Sitzung und überprüfen Sie, ob der Schlüssel H264 im Registrierungspfad erstellt wurde. Wenn ja, wird die H.264-Codierung verwendet.

```
/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

### Sicherstellen, dass die Hardwarecodierung für 3D Pro verwendet wird


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3D Pro-Hardwarecodierung ist standardmäßig deaktiviert. Aktivieren Sie die Funktion mit dem folgenden Befehl:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"HardwareEncoding" -d "0x00000001" --force
```

Starten Sie die Sitzung und überprüfen Sie den Wert von "HardwareEncoding" im Registrierungspfad. 0 bedeutet, Hardwarecodierung wird nicht verwendet, 1 bedeutet, Hardwarecodierung wird verwendet.

```
/opt/Citrix/VDA/bin/ctxreg list -k
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

Verwenden Sie den Befehl unten, um die Sitzungs-ID abzufragen:

```
/opt/Citrix/VDA/bin/ctxqsession
```

### Anpassen der Desktopumgebung für alle Benutzer

Der Linux-VDA ermöglicht es dem Benutzer nicht, bei der Anmeldung die Desktopumgebung auszuwählen. Um dieses Problem zu umgehen, kann der Benutzer eine Datei (z. B. .xsession) für die Linux-Distribution konfigurieren, um die Standarddesktopumgebung für alle Benutzer festzulegen. Weitere Informationen finden Sie in der Dokumentation zur Linux-Distribution.

Festlegen von KDE als Standardumgebung:

```
#! /usr/bin/env bash
exec startkde
```

Festlegen von GNOME als Standarddesktopumgebung:

```
#! /usr/bin/env bash
exec gnome-session
```

### Überprüfen Sie, ob die Linux-Maschine richtig vorbereitet wurde

Die häufigsten Probleme sind das Ergebnis einer Fehlkonfiguration der Linux-Maschine, hauptsächlich im Netzwerkbereich, bei der Konfiguration des NTP-Zeitservers oder der Active Directory-Domänenmitgliedschaft. Durch das Beheben der Konfigurationsprobleme der Linux-Maschine werden die Probleme mit der VDA-Software auch oft behoben.

### Konfigurieren der Protokollierung und der Ablaufverfolgung

Der Broker Agent und der HDX-Dienst protokollieren in Syslog. Citrix Support bietet Tools, die weitere Ablaufverfolgung während eines Supportanrufs aktivieren können.

### HDX-Dienstprotokollierung

Der HDX-Dienst protokolliert in Syslog und es ist keine weitere Konfiguration erforderlich.

### Broker Agent-Protokollierung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Der Broker Agent (auch ctxvda-Dienst) schreibt Protokolldaten per Netzwerk-Sockets in Syslog. Dies ist möglicherweise nicht vorkonfiguriert. Die folgende Konfiguration ist erforderlich, damit der Broker Agent in Syslog protokolliert:

Bearbeiten Sie die Datei /etc/rsyslog.conf und fügen Sie die folgenden Zeilen hinzu:

```
$ModLoad imudp

$UDPServerRun 514
```

Speichern und schließen Sie die Datei rsyslog.conf. Starten Sie den Dienst rsyslog neu, damit die Änderungen wirksam werden:

```
sudo /sbin/service rsyslog restart
```

### Lösungsansätze, wenn HDX-Sitzungen nicht starten

Stellen Sie sicher, dass keine verwaisten Prozesse vorhanden sind, die möglicherweise den Start neuer Sitzungen verhindern:

```
sudo pkill -9 ctxhdx

sudo pkill -9 ctxgfx

sudo pkill -9 ctxlogin

sudo pkill -9 ctxvfb
```

Starten Sie die Linux VDA-Dienste neu und versuchen Sie, die Verbindung herzustellen.

### Überprüfen von Besitz und Berechtigungen für Schlüsselverzeichnisse und Dateien

Überprüfen Sie den Dateibesitz und die Berechtigungen für die folgenden Verzeichnisse und Dateien:

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

### HDX 3D Pro - Probleme bei der Darstellungsaktualisierung bei mehreren Monitoren

Wenn beim Verwenden mehrerer Monitore Probleme bei der Darstellungsaktualisierung auf den sekundären Monitoren auftreten, prüfen Sie, ob die NVIDIA GRID-Lizenz verfügbar ist.

### Audio ist nicht hörbar

Stellen Sie sicher, dass die Lautstärkesteuerung auf dem Gerät, auf dem Citrix Receiver ausgeführt wird, und dem Linux-Desktop nicht stummgeschaltet oder leise ist.

Stellen Sie sicher, dass Audio auf dem Linux VDA aktiviert ist. Verwenden Sie das Tool ctxreg, um den Wert des Konfigurationselements fDisableCam abzufragen:

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

Der Wert 0x1 bedeutet, dass Audio deaktiviert ist. Sie aktivieren Audio, indem Sie fDisableCam auf 0x0 festlegen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

Wenn Audio immer noch nicht hörbar ist, prüfen Sie, ob die Citrix Audiosenke von Pulseaudio geladen wird. Das PulseAudio-Modul wird zu Beginn der Sitzung in den Pulseaudio-Daemon geladen. Überprüfen Sie mit dem Tool pacmd, ob die Citrix Audiosenke geladen ist:

```
pacmd list-sinks
```

Wenn die Citrix Audiosenke geladen ist, wird Folgendes ausgegeben:

```
name:

driver:
```

Wenn die Citrix Audiosenke nicht geladen ist, beenden Sie den ctxaudio-Prozess und starten Sie ihn neu.

### Audio wird nicht aufgezeichnet

Stellen Sie sicher, dass Audio auf dem Linux VDA und Audioaufzeichnung auf dem ICA-Client aktiviert sind. Wenn immer noch kein Audio aufgezeichnet wird, prüfen Sie, ob die Citrix Audioquelle von Pulseaudio geladen wird. Wenn Audioaufzeichnung auf dem ICA-Client aktiviert ist, wird das PulseAudio-Modul beim Sitzungsstart in den Pulseaudio-Daemon geladen. Überprüfen Sie mit dem Tool pacmd, ob die Citrix Audioquelle geladen ist:

```
pacmd list-sources
```

Wenn die Citrix Audioquelle geladen ist, wird Folgendes ausgegeben:

```
name:

driver:
```

Wenn die Citrix Audioquelle nicht geladen ist, beenden Sie den ctxaudio-Prozess und starten Sie ihn neu.

### Fehler beim Drucken

Sie können verschiedene Elemente überprüfen, wenn der Druckvorgang nicht richtig funktioniert. Der Druck-Daemon ist ein pro Sitzung ausgeführter Vorgang und sollte während der Dauer der Sitzung ausgeführt werden. Prüfen Sie, ob der Druck-Daemon ausgeführt wird.

```
ps –ef | grep ctxlpmngt
```

Wenn der ctxlpmngt-Vorgang nicht ausgeführt wird, starten Sie ctxlpmngt manuell über eine Befehlszeile.

Wenn das Drucken immer noch nicht funktioniert, überprüfen Sie als nächstes das CUPS-Framework. Der ctxcups-Dienst ist für die Druckerverwaltung und kommuniziert mit dem Linux CUPS-Framework. Dies ist ein Prozess pro Maschine und kann mit folgendem Befehl überprüft werden:

```
service ctxcups status
```

Wenn der Dienst nicht ausgeführt wird, starten Sie ihn manuell:

```
service ctxcups start
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Zusätzliches Protokoll für CUPS

Als Komponente des Linux-VDA ist die Methode zum Abrufen des Protokolls einer Druckkomponente anderen Komponenten ähnlich.

Bei Red Hat sind einige zusätzliche Schritte erforderlich, um die CUPS-Dienstdatei zu konfigurieren. Andernfalls werden einige Protokolle nicht in hdx.log protokolliert.

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
```

Das vollständige Druckprotokoll sollte mit dieser Konfiguration nur bei einem Problem abgerufen werden. Normalerweise wird diese Konfiguration nicht empfohlen, da sie die CUPS-Sicherheit verletzt.

### Druckausgabe ist fehlerhaft

Eine fehlerhafte Ausgabe kann durch einen nicht kompatiblen Druckertreiber verursacht werden. Pro Benutzer ist eine Treiberkonfiguration verfügbar und kann durch das Bearbeiten der Konfigurationsdatei ~/.CtxlpProfile konfiguriert werden.

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
```

Das Feld printername enthält den Namen des aktuellen Clientstandarddruckers. Dieser Wert ist schreibgeschützt und darf nicht bearbeitet werden.

> **Important**
>
> Nehmen Sie nicht gleichzeitig Eingaben in die Felder **ppdpath**, **model** und **drivertype** vor, da nur eines für den zugeordneten Drucker wirksam ist.

Wenn der universelle Druckertreiber mit dem Clientdrucker nicht kompatibel ist, kann das Modell des nativen Druckertreibers mit der Option model= konfiguriert werden. Der aktuelle Modellname des Druckers kann mit dem Befehl lpinfo gefunden werden.

```
lpinfo –m

...
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...

Das Modell kann dann passend für den Drucker festgelegt werden:

Model=xerox/ph3115.ppd.gz

Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, kann der ppd-Dateipfad für den nativen Druckertreiber konfiguriert werden. Der ppdpath-Wert ist der absolute Pfad der nativen Druckertreiberdatei.

Beispielsweise ist ein ppd-Treiber unter /home/tester/NATIVE_PRINTER_DRIVER.ppd vorhanden.

ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd

Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Diese können als Treibertyp konfiguriert werden, wenn kein nativer Druckertreiber verfügbar ist.

Beispiel: Der Standarddruckertreibertyp des Client ist PCL5.

drivertype=pcl5

> **Hinweis**
>
> Citrix Receiver für Mac und Citrix Receiver für Linux unterstützen nur PostScript-Drucker, daher sind die universellen Druckertreiber PCL5 und PCL6 nicht relevant. In dieser Situation muss ppdpath oder das Modell des nativen Druckertreibers auf einen Nicht-PostScript-Drucker festgelegt werden.

### CDM funktioniert nicht

Das CDM-Feature enthält einen Daemonprozess (ctxcdmd). Wenn beim CDM-Feature ein Fehler auftritt, starten Sie die Linux VDA-Maschine neu und überprüfen Sie, ob der Daemon richtig gestartet wurde:

```
Ps -lef | grep ctxcdmd
```

Die Dateibenennung im zugeordneten Laufwerk sollte den Benennungsregeln für VDA und Receiver entsprechen.

# Bekannte Probleme

### Zustand der Feststelltaste in Citrix Receiver für Android kann beim Sitzungsroaming umgekehrt werden

Der Zustand der Feststelltaste kann aufgehoben werden, wenn über eine vorhandene Verbindung Roaming zu Citrix Receiver für Android erfolgt. Verwenden Sie als Workaround die Umschalttaste auf der erweiterten Tastatur, um zwischen Groß- und Kleinbuchstaben zu wechseln.

### Tastenkombinationen mit der Alt-Taste funktionieren nicht immer, wenn Sie mit Citrix Receiver für Mac eine

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

### Verbindung zu einem Linux VDA herstellen

Citrix Receiver für Mac sendet standardmäßig für die linke und die rechte Alt-Taste den Befehl "Alt Gr". Sie können dies in den Citrix Receiver-Einstellungen ändern, die Ergebnisse sind jedoch je nach Anwendung unterschiedlich.

### Neuere X-Clientbibliotheken können Tastaturzuordnungsprobleme unter SuSE Linux Enterprise Desktop 11 verursachen

Neuere Versionen der xorg-x11-libX11-Pakete unter SuSE Linux Enterprise Desktop 11 haben u. U. Probleme beim Ändern der Tastaturzuordnung, was zu Problemen bei der Tastaturfunktionalität in einer HDX-Sitzung führen kann. Diese Situation kann auftreten, wenn die installierte Version der Pakete im Bereich 7.4-5.11.11.1 bis 7.4-5.11.15.1 liegt.

Führen Sie als Workaround ein Rollback auf die SP3-Version des xorg-x11-libX11-Pakets durch. Änderungen der Tastaturzuordnung funktionieren dann normal. Beispiel:

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm – i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

Führen Sie das Rollback aus, bevor ein Benutzer sich an der Maschine anmeldet. Wenn dies während einer aktiven Sitzung erfolgt, werden die Einstellungen nicht wirksam, bis der Benutzer sich das nächste Mal anmeldet.

Wenn Sie ein Upgrade von SP3 ausführen, können die oben angegebenen xorg-x11-libX11-Pakete mit der aktuell installierten Version verknüpft werden, sodass sie während des Upgrades nicht geändert werden. Führen Sie vor dem Upgrade folgende Prozesse aus und fahren Sie dann normal mit dem Upgrade fort:

```
zypper al xorg-x11-libX11

zypper al xorg-x11-libX11-32bit
```

### Beim Verwenden von Linux VDA mit einem Delivery Controller von XenDesktop-Version 7.1 können Sitzungsstarts lange dauern

Der langsame Start wird durch CGP-Einstellungen in der ICA-Datei verursacht, die vom XD 7.1 Delivery Controller erstellt wurde. Wenn diese Einstellungen vorhanden sind, versucht Citrix Receiver, eine Verbindung über TCP-Port 2598 herzustellen. Entsprechend den Standardfirewalleinstellungen auf einigen Linux-Distributionen, z. B. SLED 12, werden die TCP SYN-Pakete abgelegt, was zu einem Timeout und dem langen Sitzungsstart führt. Konfigurieren Sie als Workaround die Firewall auf dem Linux VDA so, dass das TCP SYN-Paket am Port 2598 abgelehnt wird. Dieses Problem wurde in neueren Versionen des Delivery Controllers behoben.

### Fehlschlagen der Registrierung, wenn der Linux VDA der Domäne wieder hinzugefügt wird

Wenn ein Linux VDA der Domäne wieder hinzugefügt und ein neuer Satz Kerberos-Schlüssel generiert wird, kann der Broker unter bestimmten Umständen keinen Sicherheitskontext mit dem VDA herstellen. Oft ist der Grund, dass der Broker ein veraltetes zwischengespeichertes VDA-Dienstticket verwendet, das auf dem vorherigen Kerberos-Schlüsselsatz basiert. Der VDA kann zwar eine Verbindung mit dem Broker herstellen, jedoch kann der Broker keinen Sicherheitskontext zum VDA herstellen. Normalerweise schlägt die VDA-Registrierung dann fehl.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dieses Problem löst sich irgendwann von selber, wenn das VDA-Dienstticket abläuft und erneuert wird, jedoch haben Diensttickets oft eine lange Lebensdauer. Dabei kann es sich um Stunden handeln.

Sie lösen das Problem, indem Sie den Ticketcache des Brokers leeren. Starten Sie den Broker neu oder führen Sie als Administrator auf dem Broker folgenden Befehl an einer Eingabeaufforderung aus:

```
klist -li 0x3e4 purge
```

Damit werden alle Diensttickets im LSA-Cache des Netzwerkdienstprinzipals gelöscht, unter dem der Citrix Brokerdienst ausgeführt wird. Es werden jedoch auch Diensttickets für andere VDAs und möglicherweise andere Dienste entfernt. Dies ist aber kein Problem, die Diensttickets werden bei Bedarf einfach erneut vom KDC geladen.

### Bei der Verwendung von HDX 3D Pro mit GNOME fehlt das Symbol zum Sperren des Bildschirms

Wenn die NVIDIA Grid-Treiber aktiv sind, ist der Gnome Desktop Manager (GDM) nicht aktiv und die GDM-Funktion zum Sperren des Bildschirms ist nicht verfügbar.

### Plug-n-Play von Audio wird nicht unterstützt

Audioaufnahmegeräte sollten mit der Clientmaschine verbunden sein, bevor Sie mit dem Aufzeichnen von Audio in der ICA-Sitzung beginnen. Wenn ein Gerät angeschlossen wird, nachdem die Audioaufzeichnungsanwendung gestartet wurde, reagiert die Anwendung u. U. nicht mehr. Wenn dieses Problem auftritt, starten Sie die Anwendung neu. Ein ähnliches Problem kann auftreten, wenn Sie ein Aufzeichnungsgerät während der Aufzeichnung entfernen.

### Audiostörungen

Bei Windows 10 Receiver können während der Aufzeichnung Audiostörungen auftreten.

### CTXPS-Treiber ist mit einigen PLC-Druckern nicht kompatibel

Wenn Sie Druckausgabestörungen bemerken, legen Sie als Druckertreiber den nativen Druckertreiber des Herstellers fest.

### Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Clientdrucker drucken, wird die zu druckende Datei über die Serververbindung übertragen. Bei langsamen Verbindungen kann dies sehr lange dauern.

### Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen werden angezeigt

Linux hat nicht das gleiche Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Durch Ändern der CUPS-Konfigurationsdatei /etc/cups/cupsd.conf kann der Administrator diese Benachrichtigungen deaktivieren.

Suchen Sie den aktuellen, in der Datei konfigurierten Richtliniennamen.

```
DefaultPolicy default
```

Wenn der Richtlinienname "default ist, fügen Sie die folgenden Zeilen im XML-Block der Standardrichtlinie hinzu.

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ...

Require user @OWNER

Order deny,allow

Order deny,allow

# Glossar

Broker: XenDesktop-Komponente, die für die Vermittlung von HDX-Sitzungen auf den verschiedenen VDAs in einer XenDesktop-Bereitstellung verantwortlich ist. Er wird auch als DDC oder XenDesktop Controller bezeichnet.

Broker Agent: Komponente auf der Linux VDA-Maschine, die den Desktop bereitstellt. Der Broker Agent kommuniziert mit dem Broker und ermöglicht die Vermittlung von Sitzungen. Er besteht aus zwei Hauptkomponenten: dem VDA-Dienst und dem HDX-Dienst.

Citrix Director: Citrix Helpdesk-/Supportkonsole zum Überwachen und Steuern von XenDesktop-VDAs.

Citrix Studio: Citrix Verwaltungskonsole zum Konfigurieren von XenDesktop.

DDC: XenDesktop Desktop Delivery Controller. Wird auch als Broker oder Delivery Controller bezeichnet.

FQDN: Vollqualifizierter Domänenname (Fully Qualified Domain Name)

HDX: High Definition Experience-Protokoll. Wurde früher als Citrix ICA-Protokoll bezeichnet.

HDX-Dienst: Der Linux-Dienst (ctxhdx), der mit dem HDX-Protokoll eine Remoteverbindung zum virtuellen Linux-Desktop herstellt. Er kommuniziert mit dem VDA-Dienst zum Vermitteln von Sitzungen.

RHEL: Red Hat Enterprise Linux. Eine kommerzielle Linux-Distribution von Red Hat.

SLED: SUSE Linux Enterprise Desktop. Eine kommerzielle Linux-Distribution von Novell.

SLES: SUSE Linux Enterprise Server. Eine kommerzielle Linux-Distribution von Novell.

VDA: Virtual Delivery Agent.

VDA-Dienst: Der Linux-Dienst (ctxvda), der mit dem Broker kommuniziert, um das Vermitteln von Sitzungen zu ermöglichen. Zudem kommuniziert er mit dem HDX-Dienst für die Bereitstellung von Remotesitzungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren von VDAs mit SUSE Linux

Jul 08, 2016

Sie können virtuelle Linux-Desktops auf der Basis einer SUSE-Distribution erstellen. Bereiten Sie die Linux-VMs vor, installieren Sie die neue Linux-VDA-Software darauf, konfigurieren Sie den Delivery Controller und stellen Sie die Desktops den Benutzern mit Studio zur Verfügung.

Weitere Informationen finden Sie in diesem Artikel.

> **Hinweis**
>
> Die in diesem Artikel beschriebenen Linux-Shellbefehle wurden für die GNU Bash-Shell verifiziert.

Der Artikel enthält die folgenden Abschnitte:


- Systemanforderungen
- Konfigurieren von Delivery Controllern
- Vorbereiten von Linux-Maschinen für die VDA-Installation
- Konfigurieren eines Linux-Maschinenkatalogs und einer Bereitstellungsgruppe
- Installieren der Linux VDA-Software
- Ausführen der VDA-Software
- Deinstallieren der Linux VDA-Software
- Problembehandlung
- Bekannte Probleme
- Glossar


# Systemanforderungen

Die folgenden Linux-Distributionen werden vom Linux Virtual Desktop unterstützt:

- SUSE Linux Enterprise:
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2
- CentOS Linux
  - CentOS 6.7
  - CentOS 7.2


© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Hinweis**
>
> In allen Fällen wird die Prozessorarchitektur x86-64 unterstützt.

Die folgenden Versionen von XenDesktop werden vom Linux VDA unterstützt:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Die Konfiguration von Linux VDAs ist etwas anders als die von Windows VDAs. Alle Delivery Controller-Farmen können jedoch Windows- und Linux-Desktops vermitteln.

> **Hinweis**
>
> Der Linux VDA ist nicht mit XenDesktop 7.0 oder früheren Versionen kompatibel.

Die folgenden Versionen von Citrix Receiver werden unterstützt:

- Citrix Receiver für Windows Version 4.4 oder höher (dies entspricht v14.4 von wfica32.exe)
- Citrix Receiver für Linux Version 13.3 oder höher
- Citrix Receiver für Mac OSX Version 12.1 oder höher
- Citrix Receiver für Android Version 3.8 oder höher
- Citrix Receiver für iOS Version 6.1.4 oder höher
- Citrix Receiver für Chrome/HTML5 Version 2.0 (nur über Access Gateway)

Die folgenden Hypervisors werden zum Hosten von Linux VDA Gast-VMs unterstützt:

- XenServer
- VMware ESX und ESXi
- Microsoft Hyper-V

Bare-Metal-Hosting wird ebenfalls unterstützt.

> **Tipp**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation des Herstellers Ihres Hypervisors.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die folgenden Active Directory-Integrationspakete oder -produkte werden vom Linux VDA unterstützt:

- Samba Winbind
- Quest Authentication Services v4.1 oder höher
- Centrify DirectControl

> **Tipp**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation des Herstellers Ihres Active Directory-Integrationspakets.

# Konfigurieren von Delivery Controllern

XenDesktop 7.7 oder höher enthält die erforderlichen Änderungen für Linux Virtual Desktop und für frühere Versionen ist ein Hotfix oder Updateskript erforderlich. Anleitungen zur Installation und Überprüfung finden Sie in diesem Abschnitt.

Wenden Sie bei XenDesktop 7.6 SP2 das Hotfix Update 2 an, um den Broker für Linux Virtual Desktops zu aktualisieren. Hotfix Update 2 ist hier verfügbar:

- CTX142438: Hotfix Update 2 - für Delivery Controller 7.6 (32 Bit) – Englisch
- CTX142439: Hotfix Update 2 - für Delivery Controller 7.6 (64 Bit) – Englisch

Für frühere XenDesktop-Versionen ist das PowerShell-Skript **Update-BrokerServiceConfig.ps1** verfügbar, mit dem die Konfiguration des Brokerdiensts aktualisiert wird. Es ist im folgenden Paket verfügbar:

- citrix-linuxvda-scripts-1.3.0.zip

Führen Sie die folgenden Schritte auf *jedem* Delivery Controller in der Farm aus:

1. Kopieren Sie das Skript **Update-BrokerServiceConfig.ps1** auf den Delivery Controller.
2. Öffnen Sie als lokaler Administrator eine Windows PowerShell-Konsole.
3. Navigieren Sie zu dem Ordner, der das Skript enthält.
4. Führen Sie das Skript aus:

```
.\Update-BrokerServiceConfig.ps1
```

> **Hinweis**
>
> Standardmäßig verhindert die Konfiguration von PowerShell das Ausführen von PowerShell-Skripts. Wenn das Skript nicht ausgeführt wird, müssen Sie möglicherweise die PowerShell-Ausführungsrichtlinie ändern und das Skript erneut ausführen:
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```

Das Skript **Update-BrokerServiceConfig.ps1** aktualisiert die Brokerdienstkonfigurationsdatei mit neuen WCF-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Endpunkten, die der Linux VDA erfordert, und startet den Brokerdienst neu. Das Skript bestimmt den Speicherort der Brokerdienstkonfigurationsdatei automatisch. Im selben Verzeichnis wird ein Backup der ursprünglichen Konfigurationsdatei mit der Erweiterung **.prelinux** angelegt.

Diese Änderungen haben keine Auswirkungen auf das Brokering von Windows VDAs, die dieselbe Delivery Controller-Farm verwenden. Auf diese Weise kann eine einzige Controller-Farm Sitzungen für Windows und Linux VDAs nahtlos verwalten und vermitteln.

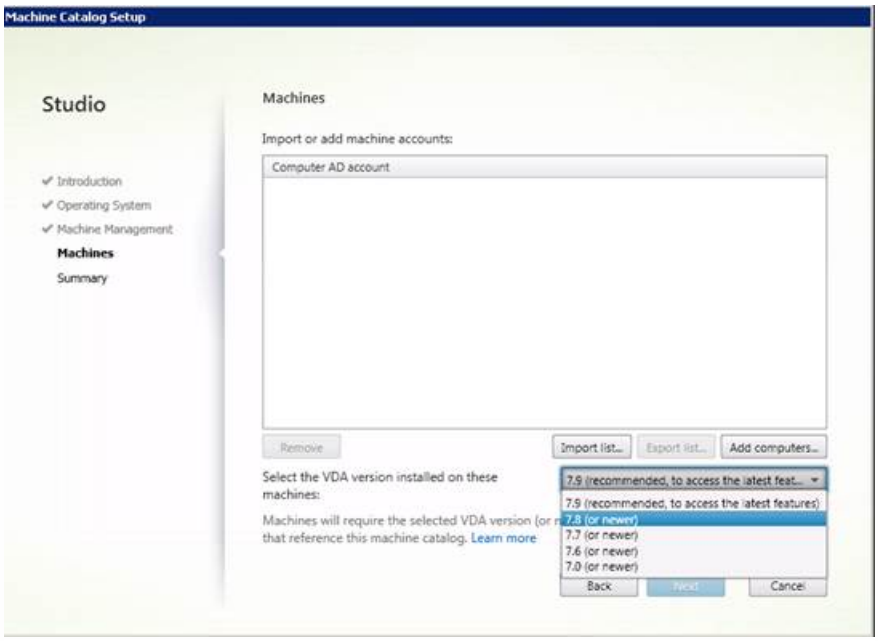
Überprüfen Sie, ob die Zeichenfolge **EndpointLinux** fünf Mal in der Datei angezeigt wird, um zu bestätigen, dass die erforderlichen Konfigurationsänderungen auf einen Delivery Controller angewendet wurden:

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

An der Windows-Eingabeaufforderung müssen Sie als lokaler Administrator angemeldet sein:

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config
```

> **Important**
>
> In Version 1.3 ist der Broker-Agent des Linux-VDAs auf XenApp/XenDesktop 7.8 festgelegt. Wird jedoch ein Maschinenkatalog über den Bildschirm zum Einrichten eines Maschinenkatalogs von Studio hinzugefügt, wird der Standardwert automatisch auf Version 7.9 festgelegt. Sie müssen die Version des installierten VDAs explizit auf **7.8 (oder höher)** festlegen (siehe Abbildung unten).




# Vorbereiten einer Linux-Maschine für die VDA-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installation

Mit dem SUSE Linux Enterprise YaST-Tool können alle Aspekte des Betriebssystems konfiguriert werden.

Starten des textbasierten YaST-Tools:

```
su -
yast
```

Sie können auch das YaST-Tool mit Benutzeroberfläche starten:

```
su -
yast2 &
```

In den folgenden Abschnitten finden Sie Informationen zum Konfigurieren der verschiedenen Netzwerkeinstellungen und Dienste, die der Linux VDA verwendet. Die Konfiguration des Netzwerks sollte mit dem YaST-Tool ausgeführt werden und nicht mit anderen Methoden wie Network Manager. Die Anleitungen beziehen sich auf das YaST-Tool mit Benutzeroberfläche. Sie können das textbasierte YaST-Tool verwenden, aber es erfordert eine andere Navigationsweise, die hier nicht dokumentiert ist.

## Konfigurieren von Hostnamen und DNS

1. Öffnen Sie "YaST Network Settings".
2. Nur in SLED 12: Ändern Sie auf der Registerkarte **Global Options** die Einstellung unter **Network Setup Method** in **Wicked Service**.
3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Deaktivieren Sie das Kontrollkästchen **Change hostname via DHCP**.
5. Aktivieren Sie das Kontrollkästchen **Assign Hostname to Loopback IP**.
6. Geben Sie die folgenden Informationen entsprechend Ihrer Netzwerkeinstellungen an:

- Hostname: Geben Sie den DNS-Hostnamen der Maschine an.
- Domain Name: Geben Sie den DNS-Domänennamen der Maschine an.
- Name Server: Geben Sie die IP-Adresse des DNS-Servers an. Dies ist normalerweise die IP-Adresse des Active Directory-Domänencontrollers.
- Domain Search list: Geben Sie den DNS-Domänennamen an.

### Hinweis

Der Linux VDA unterstützt derzeit keine abgeschnittenen NetBIOS-Namen, daher darf der Hostname nicht länger als 15 Zeichen sein.

### Tipp

Verwenden Sie nur Buchstaben (a-z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Symbole. Hostnamen sollten nicht mit einer Zahl beginnen und nicht mit einem Bindestrich enden.

## Deaktivieren von Multicast-DNS

In SLED ist standardmäßig Multicast-DNS (MDNS) aktiviert, was zu inkonsistenten Ergebnissen bei der Namensauflösung führen kann. In SLES ist MDNS nicht standardmäßig aktiviert, daher ist keine Aktion erforderlich.

Sie deaktivieren MDNS, indem Sie /etc/nsswitch.conf bearbeiten und folgende Zeile ändern:

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

In:

```
hosts: files dns
```

## Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

```
hostname
```

Nur der Hostname der Maschine sollte zurückgegeben werden und nicht der vollqualifizierte Domänenname (FQDN).

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

```
hostname -f
```

Der FQDN der Maschine sollte zurückgegeben werden.

## Überprüfen von Namensauflösung und Diensterreichbarkeit

Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den XenDesktop Delivery Controller:

nslookup **domain-controller-fqdn**

ping **domain-controller-fqdn**

nslookup **delivery-controller-fqdn**

ping **delivery-controller-fqdn**

Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den XenDesktop Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem NTP-Dienst verwaltet werden. Möglicherweise müssen einige Änderungen an den NTP-Standardeinstellungen vorgenommen werden:

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

1. Öffnen Sie "YaST NTP Configuration" und wählen Sie die Registerkarte **General Settings** aus.
2. Aktivieren Sie im Abschnitt "Start NTP Daemon" das Kontrollkästchen **Now and on Boot**.
3. Wählen Sie das Element **Undisciplined Local Clock (LOCAL)** aus, wenn es vorhanden ist, und klicken Sie auf **Delete**.
4. Fügen Sie einen Eintrag für einen NTP-Server hinzu, indem Sie auf **Add** klicken.
5. Wählen Sie unter **Server Type** den Servertyp aus und klicken Sie auf **Next**.
6. Geben Sie den DNS-Namen des NTP-Servers in das Adressfeld ein. Dieser Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
7. Lassen Sie das Feld "Options" unverändert.
8. Klicken Sie auf **Test**, um zu prüfen, ob der NTP-Dienst erreichbar ist.
9. Klicken Sie in den folgenden Fenstern auf **OK**, um die Änderungen zu speichern.

> **Hinweis**
>
> Wenn der NTP-Daemon in SLES 12-Implementierungen nicht startet, ist dies möglicherweise auf ein bekanntes SUSE-Problem mit AppArmor-Richtlinien zurückzuführen. Weitere Informationen und eine Lösung des Problems finden Sie hier.

Die Linux VDA-Software für Suse Linux Enterprise ist von den folgenden Paketen abhängig:

- PostgreSQL
  - SLED/SLES 11: Version 9.1 oder höher
  - SLED/SLES 12: Version 9.3 oder höher
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 oder höher
- Cups
  - SLED/SLES 11: Version 1.3.7 oder höher
  - SLED/SLES 12: Version 1.6.0 oder höher
- Foomatic-Filter
  - SLED/SLES 11: Version 3.0.0 oder höher
  - SLED/SLES 12: Version 1.0.0 oder höher
- ImageMagick
  - SLED/SLES 11: Version 6.4.3.6 oder höher
  - SLED/SLES 12: Version 6.8 oder höher

## Hinzufügen von Repositorys

Einige der erforderlichen Pakete sind nicht in allen SUSE Linux Enterprise-Repositorys verfügbar:

- SLED 11: PostgreSQL ist für SLES 11, aber nicht für SLED 11 verfügbar.
- SLES 11: OpenJDK und OpenMotif sind für SLED 11, aber nicht SLES 11 verfügbar.
- SLED 12: PostgreSQL ist für SLES 12, aber nicht für SLED 12 verfügbar. ImageMagick ist mit dem SLE 12 SDK ISO oder dem Online-Repository verfügbar.
- SLES 12: Alle Pakete sind verfügbar. ImageMagick ist mit dem SLE 12 SDK ISO oder dem Online-Repository verfügbar.

Laden Sie fehlende Pakete für die Edition, die Sie installieren, vom Medium für die alternative SLE-Edition herunter. Das bedeutet, für SLED können Sie fehlende Pakete vom SLES-Medium installieren und für SLES können Sie fehlende Pakete


© 1999-2017 Citrix Systems, Inc. All rights reserved.

vom SLED-Medium installieren. Mit der unten beschriebenen Methode werden die ISO-Dateien und Repositorys sowohl für SLED als auch SLES bereitgestellt.

| | |
|---|---|
| SLED 11 | sudo mkdir -p /mnt/sles<br>sudo mount -t iso9660 \<br>path-to-iso/SLES-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sles<br>sudo zypper ar -f /mnt/sles sles |
| SLES 11 | sudo mkdir -p /mnt/sled<br>sudo mount -t iso9660 \<br>path-to-iso/SLED-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sled<br>sudo zypper ar -f /mnt/sled sled |
| SLED 12 | sudo mkdir -p /mnt/sles<br>sudo mount -t iso9660 \<br>path-to-iso/SLES-12-DVD-x86_64-GM-DVD1.iso /mnt/sles<br>sudo zypper ar -f /mnt/sles sles |
| SLED/SLES 12 | sudo mkdir -p /mnt/sdk<br>sudo mount -t iso9660 \<br>path-to-iso/SLE-12-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk<br>sudo zypper ar -f /mnt/sdk sdk |

## Installieren des Kerberos-Clients

Installieren Sie den Kerberos-Client für die gegenseitige Authentifizierung des Linux VDA und der XenDesktop Controller:

```
sudo zypper install krb5-client
```

Die Kerberos-Clientkonfiguration ist abhängig von der verwendeten Active Directory-Integrationsmethode, die später beschrieben wird.

## Installieren von OpenJDK

Der Linux VDA ist von OpenJDK 1.7.0 abhängig.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Tipp**
>
> Stellen Sie zum Vermeiden von Problemen sicher, dass nur die OpenJDK-Version 1.7.0 installiert ist. Entfernen Sie alle anderen auf dem System vorhandenen Java-Versionen.

| | |
|---|---|
| SLED | Unter SLED sollte Java Runtime Environment mit dem Betriebssystem installiert worden sein. Überprüfen Sie dies mit folgenden Befehl:<br>sudo zypper info java-1_7_0-openjdk<br>Aktualisieren Sie auf die aktuelle Version, wenn der Status als veraltet gemeldet wird:<br>sudo zypper update java-1_7_0-openjdk<br>Überprüfen Sie die Java-Version:<br>java -version |
| SLES | Unter SLES muss Java Runtime Environment installiert werden:<br>sudo zypper install java-1_7_0-openjdk<br>Überprüfen Sie die Java-Version:<br>java -version |

## Installieren von PostgreSQL

| | |
|---|---|
| SLED/SLES 11 | Installieren Sie die Pakete:<br>sudo zypper install libecpg6<br>sudo zypper install postgresql?init<br>sudo zypper install postgresql91<br>sudo zypper install postgresql91?server<br>sudo zypper install postgresql?jdbc<br>Nach der Installation sind einige Schritte erforderlich, um den Datenbankdienst zu initialisieren und sicherzustellen, dass PostgreSQL beim Booten startet:<br>sudo /sbin/insserv postgresql<br>sudo /etc/init.d/postgresql restart |
| | Installieren Sie die Pakete: |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| SLED/SLES 12 | sudo zypper install postgresql-init<br>sudo zypper install postgresql93-server<br>sudo zypper install postgresql-jdbc<br>Nach der Installation sind Schritte erforderlich, um den Datenbankdienst zu initialisieren und sicherzustellen, dass PostgreSQL beim Booten startet:<br>sudo systemctl enable postgresql<br>sudo systemctl restart postgresql<br>Datenbankdateien befinden sich unter /var/lib/pgsql/data. |

## Installieren der OpenMotif Runtime Environment

Abhängig von der Distribution benötigt der Linux VDA das motif- oder openmotif-Paket.

| | |
|---|---|
| SLED/SLES 11 | Installieren Sie das Paket:<br>sudo zypper install openmotif-libs |
| SLED/SLES 12 | Installieren Sie das Paket:<br>sudo zypper install motif |

## Installieren der Druckunterstützung

Der Linux VDA erfordert Cups- und Foomatic-Filter.

| | |
|---|---|
| SLED/SLES 11 | Installieren Sie die Pakete:<br>sudo zypper install cups<br>sudo zypper install foomatic-filters |
| SLED/SLES 12 | Installieren Sie die Pakete:<br>sudo zypper install cups<br>sudo zypper install cups-filters-foomatic-rip |

## Installieren von ImageMagick

Installieren Sie das ImageMagick-Paket:

sudo zypper install ImageMagick


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Entfernen von Repositorys

Nach der Installation der abhängigen Pakete können nun die zuvor eingerichteten Repositorys der alternativen Edition entfernt und die Bereitstellung der Medien aufgehoben werden:

| | |
|---|---|
| SLED 11 | Entfernen Sie die folgenden Pakete:<br>sudo zypper rr sles<br>sudo umount /mnt/sles<br>sudo rmdir /mnt/sles |
| SLES 11 | Entfernen Sie die folgenden Pakete:<br>sudo zypper rr sled<br>sudo umount /mnt/sled<br>sudo rmdir /mnt/sled |
| SLED 12 | Entfernen Sie die folgenden Pakete:<br>sudo zypper rr sles<br>sudo umount /mnt/sles<br>sudo rmdir /mnt/sles |
| SLED/SLES 12 | Entfernen Sie die folgenden Pakete:<br>sudo zypper rr sdk<br>sudo umount /mnt/sdk<br>sudo rmdir /mnt/sdk |

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie entsprechend der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

## Festlegen der Zeitsynchronisierung auf Citrix XenServer

Wenn das Zeitsynchronisierungsfeature auf XenServer aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und XenServer gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. Dazu muss die Hostzeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen, auf denen ein paravirtualisierter Linux-Kernel mit installierten XenServer-Tools ausgeführt

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

wird, können Sie direkt in der Linux-VM prüfen, ob das XenServer- Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Mögliche Ergebnisse:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.
- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei /proc/sys/xen/indepent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Wenn das Zeitsynchronisierungsfeature aktiviert ist, deaktivieren Sie es, indem Sie "1" in die Datei eingeben:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, bearbeiten Sie die Datei /etc/sysctl.conf und fügen Sie die folgende Zeile hinzu:

```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

```
reboot
```

Nach dem Neustart müssen Sie sicherstellen, dass die Einstellung richtig festgelegt wurde:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Der Wert "1" sollte zurückgegeben werden.

## Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Um sicherzustellen, dass die Betriebssystemzeit korrekt ist, sollten Sie das Feature zusätzlich zu den NTP-Diensten aktivieren.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integration Services** aus.
3. Stellen Sie sicher, dass **Time synchronization** ausgewählt ist.

> ### Hinweis
>
> Diese Methode unterscheidet sich von VMware und XenServer, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und der Hypervisor gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. Dazu muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie "VMware Tools".
5. Deaktivieren Sie im Bereich **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Linux-Maschinen können mit verschiedenen Methoden der Active Directory-Domäne hinzugefügt werden, die von XenDesktop für Linux unterstützt wird:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Folgen Sie den Anweisungen unten für die von Ihnen gewählte Methode.

## Samba Winbind

### Beitreten zu einer Windows-Domäne

Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Maschinen zur Domäne verfügen:

1. Öffnen Sie "YaST Windows Domain Membership".

2. Nehmen Sie die folgenden Änderungen vor:

- Legen Sie die Domäne oder Arbeitsgruppe auf den Namen der Active Directory-Domäne oder auf die IP-Adresse des Domänencontrollers fest. Stellen Sie sicher, dass die Domäne in Großbuchstaben angegeben wurde.
- Aktivieren Sie außerdem das Kontrollkästchen "Use SMB information for Linux Authentication".
- Aktivieren Sie das Kontrollkästchen "Create Home Directory on Login".
- Aktivieren Sie "Single Sign-on for SSH".
- Stellen Sie sicher, dass die Option "Offline Authentication" nicht aktiviert ist. Diese Option ist mit dem Linux VDA nicht kompatibel.

3. Klicken Sie auf OK. Wenn Sie zum Installieren einiger Pakete aufgefordert werden, klicken Sie auf "Install".

4. Wenn ein Domänencontroller gefunden wird, werden Sie gefragt, ob Sie der Domäne beitreten möchten. Klicken Sie auf "Yes".

5. Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen eines Domänenbenutzers ein, der über

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Berechtigungen zum Hinzufügen von Computern zur Domäne verfügt, und klicken Sie auf "OK".

6. Eine Erfolgsmeldung wird angezeigt.

7. Wenn Sie zum Installieren von samba- und krb5-Paketen aufgefordert werden, klicken Sie auf "Install".

YaST hat Sie möglicherweise davon unterrichtet, dass für diese Änderungen einige Dienste oder die Maschine neu gestartet werden muss. Führen Sie einen Neustart durch:

```
su -
reboot
```

### Nur für SLED/SLES 12: Reparieren des Namens für Kerberos-Anmeldeinformationscache

In SLED/SLES 12 wurde die Spezifikation für den Standardnamen des Kerberos-Anmeldeinformationscaches von FILE:/tmp/krb5cc_%{uid} in DIR:/run/user/%{uid}/krb5cc geändert. Diese neue DIR-Zwischenspeichermethode ist nicht mit dem Linux VDA kompatibel und muss manuell geändert werden. Bearbeiten Sie als Root-Benutzer die Datei /etc/krb5.conf und fügen Sie ggf. die folgende Einstellung im Abschnitt [libdefaults] hinzu:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

### Überprüfen der Domänenmitgliedschaft

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben.

Stellen Sie mit dem folgenden Samba-Befehl sicher, dass die Maschine zu einer Domäne gehört:

```
sudo net ads testjoin
```

Überprüfen Sie zusätzliche Domänen- und Computerobjektinformationen mit folgendem Befehl:

```
sudo net ads info
```

### Überprüfen der Kerberos-Konfiguration

Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:

```
sudo klist –ke
```

Daraufhin sollte die Liste der Schlüssel angezeigt werden, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl kinit aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

```
sudo kinit -k MACHINE\$@REALM
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden und das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um die Ersetzung in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

```
sudo klist
```

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

```
sudo net ads status
```

### Überprüfen der Benutzerauthentifizierung

Überprüfen Sie mit dem wbinfo-Tool, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

```
wbinfo --krb5auth=domain\\username%password
```

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sicherzustellen, dass das Winbind PAM-Modul richtig konfiguriert ist, melden Sie sich lokal mit einem Domänenbenutzerkonto an, mit dem noch nie eine Anmeldung an der Maschine vorgenommen wurde:

```
ssh localhost -l domain\\username
```

```
id -u
```

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl id -u zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung:

```
exit
```

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden.

## Quest Authentication Service

### Konfigurieren von Quest auf dem Domänencontroller

Es wird vorausgesetzt, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über Administratorrechte zum Erstellen von Computerobjekten in Active Directory verfügen.

### Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen

Für alle Domänenbenutzer, die HDX-Sitzungen auf einer Linux VDA-Maschine herstellen, führen Sie folgende Schritte aus:

1. Öffnen Sie in der Verwaltungskonsole für Active Directory-Benutzer und -Computer die Active Directory-Eigenschaften für das jeweilige Benutzerkonto.
2. Wählen Sie die Registerkarte "Unix Account" aus.
3. Aktivieren Sie das Kontrollkästchen "Unix-enabled".
4. Legen Sie "Primary GID Number" auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

> **Hinweis**
>
> Mit diesen Anleitungen können Domänenbenutzer für die Anmeldung mit der Konsole, RDP, SSH oder anderen Remotingprotokollen eingerichtet werden.

### Konfigurieren von Quest auf Linux VDA

#### Konfigurieren des VAS-Daemon

Die automatische Erneuerung von Kerberos-Tickets muss aktiviert und getrennt sein. Authentifizierung (für Offlineanmeldung) muss deaktiviert sein:

```
sudo /opt/quest/bin/vastool configure vas vasd \
                    auto-ticket-renew-interval 32400
sudo /opt/quest/bin/vastool configure vas vas_auth \
                    allow-disconnected-auth false
```

Hiermit wird das Verlängerungsintervall auf 9 Stunden (32400 Sekunden) festgelegt. Das ist eine Stunde weniger als die Standardgültigkeitsdauer (10 Stunden) eines Tickets. Bei Systemen mit einer kürzeren Gültigkeitsdauer für Kerberos-Tickets legen Sie diesen Parameter auf einen niedrigeren Wert fest.

#### Konfigurieren von PAM und NSS

Quest erfordert, dass PAM und NSS manuell konfiguriert werden, um Domänenbenutzern die Anmeldung per HDX und anderen Diensten, wie SU, SSH und RDP, zu ermöglichen. Konfigurieren von PAM und NSS:

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
```

#### Beitreten zu einer Windows-Domäne

Machen Sie die Linux-Maschine mit dem Quest-Befehl "vastool" zu einem Mitglied der Active Directory-Domäne:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der Benutzer ist ein beliebiger Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. Der Domänenname ist der DNS-Name der Domäne, z. B. example.com.

#### Überprüfen der Domänenmitgliedschaft

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Quest angemeldete Linux-Maschine zur Domäne gehört:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine zu einer Domäne gehört, wird der Domänenname zurückgegeben. Wenn sie nicht zur Domäne gehört,


© 1999-2017 Citrix Systems, Inc. All rights reserved.

wird die folgende Fehlermeldung angezeigt:

ERROR: No domain could be found.

ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm

default_realm not configured in vas.conf. Computer may not be joined to domain

### Überprüfen der Benutzerauthentifizierung

Um sicherzustellen, dass Quest Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto an, mit dem noch nie eine Anmeldung an der Maschine vorgenommen wurde:

ssh localhost -l domain\\username

id -u

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl id -u zurückgegebene UID erstellt wurde:

ls /tmp/krb5cc_uid

Stellen Sie sicher, dass die im Tickets Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

/opt/quest/bin/vastool klist

Beenden Sie die Sitzung:

exit

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden.

## Centrify DirectControl

### Beitreten zu einer Windows-Domäne

Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl **adjoin** zu einem Mitglied der Active Directory-Domäne:

su –

adjoin -w -V -u **user domain-name**

Der Parameter **user** ist ein Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern von Active Directory-Domänen zu machen. Der Parameter "domain-name" ist der Name der Domäne, der die Linux-Maschine beitritt.

### Überprüfen der Domänenmitgliedschaft

Für den XenDesktop Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

su –

adinfo

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all
```

```
adinfo –diag
```

Testen der Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten:

```
adinfo --test
```

# Konfigurieren eines Linux-Maschinenkatalogs und einer Bereitstellungsgruppe

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ist der traditionellen Windows VDA-Methode sehr ähnlich. Umfassendere Informationen zu diesen Prozessen finden Sie in der Citrix Produktdokumentation.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen, durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Windows-Serverbetriebssystem oder Serverbetriebssystem für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Windows-Desktopbetriebssystem oder Desktopbetriebssystem für ein VDI-dediziertes Desktopbereitstellungsmodell.
- Stellen Sie sicher, dass für die Maschinen keine Energieverwaltung festgelegt ist.
- Da PVS und MCS für Linux VDAs nicht unterstützt werden, wählen Sie die Bereitstellungsmethode **Anderer Dienst oder andere Technologie** (vorhandene Images).
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> ## Hinweis
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von Windows-Serverbetriebssystem oder Serverbetriebssystem wird ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von Windows-Desktopbetriebssystem oder Desktopbetriebssystem wird ein Bereitstellungsmodell für XenDesktop Einzelbenutzermaschinen bereitgestellt.

Anleitungen zum Erstellen von Maschinenkatalogen finden Sie in der Citrix Dokumentation unter der jeweiligen Version:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Frühere Versionen von XenDesktop werden nicht unterstützt.

> **Tipp**
>
> Wenn eine Maschine eine Active Directory-Domäne verlässt und ihr dann wieder beitritt, muss die Maschine aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie online in der Citrix Produktdokumentation.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Wählen Sie als Bereitstellungstyp "Desktops" aus. Linux VDA-Maschinen unterstützen keine Bereitstellung von Anwendungen.
- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

Anleitungen zum Erstellen von Bereitstellungsgruppen finden Sie in der Citrix Dokumentation unter der jeweiligen Version:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Frühere Versionen von XenDesktop werden nicht unterstützt.

# Installieren der Linux VDA-Software

Wenn bereits eine ältere Linux VDA-Version als Version 1.0 installiert ist, deinstallieren Sie diese Version, bevor Sie die neue Version installieren.

Halten Sie die Linux VDA-Dienste an:

```
sudo /sbin/service ctxvda stop
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
sudo /sbin/service ctxhdx stop
```

Deinstallieren Sie das Paket:

```
sudo rpm -e XenDesktopVDA
```

> **Important**
>
> Das Upgrade von der Tech Preview auf Version 1.0, 1.1, 1.2 und 1.3 wird nicht unterstützt.

> **Hinweis**
>
> Ab Version 1.3 wurde der Installationspfad geändert. In vorherigen Releases waren die Installationskomponenten unter **/usr/local/**. Der neue Speicherort ist **/opt/Citrix/VDA/**.
>
> Zum Ausführen eines Befehls ist der vollständige Pfad erforderlich. Alternativ können Sie **/opt/Citrix/VDA/sbin** und /opt/Citrix/VDA/bin dem Systempfad hinzufügen.

Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager:

**Für SuSE 11**:

```
sudo rpm -i XenDesktopVDA-1.3.312-1.x86_64.rpm
```

**Für SuSE 12**:

```
sudo rpm -i XenDesktopVDA-1.3.312-1.x86_64.rpm
```

Wenn Sie Version 1.1 des Linux VDA installiert haben, aktualisieren Sie die Linux VDA-Software mit dem RPM-Paketmanager:

**Für SuSE 11**:

```
sudo rpm -U XenDesktopVDA-1.3.312-1.x86_64.rpm
```

**Für SuSE 12**:

```
sudo rpm -U XenDesktopVDA-1.3.312-1.x86_64.rpm
```

> **Important**
>
> Nach dem Upgrade müssen Sie die Linux VDA-Maschine neu starten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript **ctxsetup.sh** ausführen. Wenn Sie das Paket aktualisiert haben, müssen Sie das Skript ctxsetup.sh ausführen, um das Upgrade abzuschließen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Bei Bedarf können Sie dieses Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Das Skript kann manuell mit Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausgeführt werden. Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

## Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

## Automatische Konfiguration

Bei einer automatischen Installation können die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen angegeben werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine weiteren Informationen vom Benutzer und der Installationsvorgang wird per Skript ausgeführt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N: Der Virtual Delivery Agent unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Einstellung ist normalerweise N.
- CTX_XDL_DDC_LIST = list-ddc-fqdns: Der Virtual Delivery Agent erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) von Delivery Controllern
- zur Registrierung mit einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- TX_XDL_VDA_PORT = port-number: Der Virtual Delivery Agent kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist normalerweise Port 80.
- CTX_XDL_REGISTER_SERVICE = Y | N: Der Support für Linux Virtual Desktop-Dienste wird während des Startvorgangs gestartet. Die Einstellung ist normalerweise Y.
- CTX_XDL_ADD_FIREWALL_RULES = Y | N: Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Einstellung ist normalerweise Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3: Für den Virtual Delivery Agent müssen Kerberos-Konfigurationseinstellungen von den Delivery Controllern authentifiziert werden. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt. Geben Sie die zu verwendende Active Directory-Integrationsmethode an:
  - 1 – Samba Winbind
  - 2 – Quest-Authentifizierungsdienst
  - 3 – Centrify DirectControl
- CTX_XDL_HDX_3D_PRO= Y | N: Linux Virtual Desktop unterstützt HDX 3D Pro, ein Satz Grafikbeschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Für HDX 3D Pro muss eine kompatible NVIDIA Grid-Grafikkarte installiert sein. Wenn HDX 3D Pro aktiviert ist, muss der Virtual Delivery Agent für VDI-Desktopmodus (Einzelsitzungen) konfiguriert werden (d. h. CTX_XDL_VDI_MODE=Y). Dies wird unter SUSE nicht unterstützt. Stellen Sie sicher, dass dieser Wert auf N eingestellt ist.
- CTX_XDL_VDI_MODE: =J | N: Ermöglicht die Konfiguration der Maschine als ein dediziertes

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Für HDX 3D Pro-Umgebungen muss die Einstellung Y sein. Die Einstellung ist normalerweise N.

- CTX_XDL_SITE_NAME= dns-name: Der Virtual Delivery Agent ermittelt LDAP-Server mit DNS durch die Abfrage von LDAP-Diensteinträgen. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Normalerweise ist nichts angegeben [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers: Der Virtual Delivery Agent fragt standardmäßig DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Diensteinträge ermitteln kann, können Sie eine durch Leerzeichen getrennte Liste mit LDAP-FQDNs mit LDAP-Port angeben (z. B. ad1.mycompany.com:389). Normalerweise ist nichts angegeben [none].
- CTX_XDL_SEARCH_BASE= search-base: Der Virtual Delivery Agent fragt standardmäßig LDAP mit einer Suchbasis ab, die auf den Stamm der Active Directory-Domäne festgelegt ist (z. B. DC=mycompany,DC=com). Zum Verbessern der Suchleistung kann jedoch eine Suchbasis angegeben werden (z. B. OU=VDI,DC=mycompany,DC=com). Normalerweise ist nichts angegeben [none].
- CTX_XDL_START_SERVICE = Y | N: Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Einstellung ist normalerweise Y.

> **Hinweis**
>
> HDX 3D Pro ist zurzeit nicht unter SUSE verfügbar.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Sie müssen die Option **-E** mit **sudo** angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Alternativ können alle Parameter mit einem einzigen Befehl angegeben werden:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
    CTX_XDL_DDC_LIST=list-ddc-fqdns \
    CTX_XDL_VDA_PORT=port-number \
    CTX_XDL_REGISTER_SERVICE=Y|N \
    CTX_XDL_ADD_FIREWALL_RULES=Y|N \
    CTX_XDL_AD_INTEGRATION=1|2|3 \
    CTX_XDL_HDX_3D_PRO=Y|N \
    CTX_XDL_VDI_MODE=Y|N \
    CTX_XDL_SITE_NAME=dns-name \
    CTX_XDL_LDAP_LIST=list-ldap-servers \
    CTX_XDL_SEARCH_BASE=search-base \
    CTX_XDL_START_SERVICE=Y|N \
    /opt/Citrix/VDA/sbin/ctxsetup.sh
```

## Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen u. U. entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

Entfernen von Konfigurationsänderungen:

```
sudo /usr/local/sbin/ctxcleanup.sh
```

> **Important**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

## Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in eine Konfigurationsprotokolldatei:

```
/tmp/xdl.configure.log
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

# Ausführen der VDA-Software

Wenn Sie den Linux VDA mit dem Skript ctxsetup.sh konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start
sudo /sbin/service ctxvda start
```

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx restart
sudo /sbin/service ctxvda start
```

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status
sudo /sbin/service ctxhdx status
```

# Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
rpm -q XenDesktopVDA
```

Anzeigen weiterer Details:

```
rpm –qi XenDesktopVDA
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Deinstallieren des Linux VDA-Pakets:

```
sudo rpm -e XenDesktopVDA
```

> **Hinweis**
>
> Beim Deinstallieren der Linux VDA-Software werden die damit verknüpften PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden nicht entfernt.

Dieser Abschnitt bezieht sich nicht auf das Entfernen von abhängigen Paketen einschließlich PostgreSQL.

# Problembehandlung

Linux VDA v1.3 fügt H264 und einen HardwareEncoding-Wert im Registrierungspfad HKLM\Software\Citrix\Ica\Session\\Graphics hinzu, um die Problembehandlung von Grafikproblemen, die beim VDA auftreten, zu unterstützen.

Führen Sie den folgenden Befehl aus, um die H.264-Codierung in einem Linux-VDA vor dem Start einer Sitzung anzukündigen:

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"AdvertiseH264" -d "0x00000001" --force
```

Starten Sie die Sitzung und überprüfen Sie, ob der Schlüssel H264 im Registrierungspfad erstellt wurde. Wenn ja, wird die H.264-Codierung verwendet.

```
/opt/Citrix/VDA/bin/ctxreg list -k

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

3D Pro-Hardwarecodierung ist standardmäßig deaktiviert. Aktivieren Sie die Funktion mit dem folgenden Befehl:

```
/opt/Citrix/VDA/bin/ctxreg create -k

"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v

"HardwareEncoding" -d "0x00000001" --force
```

Starten Sie die Sitzung und überprüfen Sie den Wert von "HardwareEncoding" im Registrierungspfad. 0 bedeutet, Hardwarecodierung wird nicht verwendet, 1 bedeutet, Hardwarecodierung wird verwendet.

```
/opt/Citrix/VDA/bin/ctxreg list -k
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"

Verwenden Sie den Befehl unten, um die Sitzungs-ID abzufragen:

/opt/Citrix/VDA/bin/ctxqsession

Der Linux-VDA ermöglicht es dem Benutzer nicht, bei der Anmeldung die Desktopumgebung auszuwählen. Um dieses Problem zu umgehen, kann der Benutzer eine Datei (z. B. .xsession) für die Linux-Distribution konfigurieren, um die Standarddesktopumgebung für alle Benutzer festzulegen. Weitere Informationen finden Sie in der Dokumentation zur Linux-Distribution.

Festlegen von KDE als Standardumgebung:

```
#! /usr/bin/env bash

exec startkde
```

Festlegen von GNOME als Standarddesktopumgebung:

```
#! /usr/bin/env bash

exec gnome-session
```

Die häufigsten Probleme sind das Ergebnis einer Fehlkonfiguration der Linux-Maschine, hauptsächlich im Netzwerkbereich, bei der Konfiguration des NTP-Zeitservers oder der Active Directory-Domänenmitgliedschaft. Durch das Beheben der Konfigurationsprobleme der Linux-Maschine werden die Probleme mit der VDA-Software auch oft behoben.

Der Broker Agent und der HDX-Dienst protokollieren in Syslog. Citrix Support bietet Tools, die weitere Ablaufverfolgung während eines Supportanrufs aktivieren können.

### HDX-Dienstprotokollierung

Der HDX-Dienst protokolliert vordefinierte Systemmeldungen und es ist keine weitere Konfiguration erforderlich.

### Broker Agent-Protokollierung

Der Broker Agent (auch ctxvda-Dienst) schreibt Protokolldaten per Netzwerk-Sockets in Syslog. Dies ist möglicherweise nicht vorkonfiguriert. Die folgende Konfiguration ist erforderlich, damit der Broker Agent in Syslog protokolliert:

#### SLED/SLES 11

Bearbeiten Sie die Datei /etc/syslog-ng/syslog-ng.conf und fügen Sie die folgende Zeile im Abschnitt s_sys hinzu:

```
udp(ip(127.0.0.1) port(514));
```

Speichern und schließen Sie die Datei syslog-ng.conf. Starten Sie den Dienst syslog-ng neu, um die Änderung anzuwenden:

```
sudo service syslog-ng restart
```

#### SLED/SLES 12

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Bearbeiten Sie die Datei /etc/rsyslog.conf und fügen Sie die folgenden Zeilen hinzu:

```
$ModLoad imudp
$UDPServerRun 514
```

Speichern und schließen Sie die Datei rsyslog.conf. Starten Sie den Dienst rsyslog neu, um die Änderung anzuwenden:

```
sudo service rsyslog restart
```

Stellen Sie sicher, dass keine verwaisten Prozesse vorhanden sind, die möglicherweise den Start neuer Sitzungen verhindern:

```
sudo pkill -9 ctxhdx
sudo pkill -9 ctxgfx
sudo pkill -9 ctxlogin
sudo pkill -9 ctxvfb
```

Starten Sie die Linux VDA-Dienste neu und versuchen Sie, die Verbindung herzustellen.

Überprüfen Sie den Dateibesitz und die Berechtigungen für die folgenden Verzeichnisse und Dateien:

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

Stellen Sie sicher, dass die Lautstärkesteuerung auf dem Gerät, auf dem Citrix Receiver ausgeführt wird, und dem Linux-Desktop nicht stummgeschaltet oder leise ist.

Stellen Sie sicher, dass Audio auf dem Linux VDA aktiviert ist. Verwenden Sie das Tool ctxreg, um den Wert des Konfigurationselements fDisableCam abzufragen:

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

Der Wert 0x1 bedeutet, dass Audio deaktiviert ist. Sie aktivieren Audio, indem Sie fDisableCam auf 0x0 festlegen:

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam  -d
0x00000000
```

Wenn Audio immer noch nicht hörbar ist, prüfen Sie, ob die Citrix Audiosenke von Pulseaudio geladen wird. Das PulseAudio-Modul wird zu Beginn der Sitzung in den Pulseaudio-Daemon geladen. Überprüfen Sie mit dem Tool pacmd, ob die Citrix Audiosenke geladen ist:

```
pacmd list-sinks
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn die Citrix Audiosenke geladen ist, wird Folgendes ausgegeben:

```
name:

driver:
```

Wenn die Citrix Audiosenke nicht geladen ist, beenden Sie den ctxaudio-Prozess und starten Sie ihn neu.

Stellen Sie sicher, dass Audio auf dem Linux VDA und Audioaufzeichnung auf dem ICA-Client aktiviert sind. Wenn immer noch kein Audio aufgezeichnet wird, prüfen Sie, ob die Citrix Audioquelle von Pulseaudio geladen wird. Wenn Audioaufzeichnung auf dem ICA-Client aktiviert ist, wird das PulseAudio-Modul beim Sitzungsstart in den Pulseaudio-Daemon geladen. Überprüfen Sie mit dem Tool pacmd, ob die Citrix Audioquelle geladen ist:

```
pacmd list-sources
```

Wenn die Citrix Audioquelle geladen ist, wird Folgendes ausgegeben:

```
name:

driver:
```

Wenn die Citrix Audioquelle nicht geladen ist, beenden Sie den ctxaudio-Prozess und starten Sie ihn neu.

Sie können verschiedene Elemente überprüfen, wenn der Druckvorgang nicht richtig funktioniert. Der Druck-Daemon ist ein pro Sitzung ausgeführter Vorgang und sollte während der Dauer der Sitzung ausgeführt werden. Prüfen Sie, ob der Druck-Daemon ausgeführt wird.

```
ps –ef | grep ctxlpmngt
```

Wenn der ctxlpmngt-Vorgang nicht ausgeführt wird, starten Sie ctxlpmngt manuell über eine Befehlszeile.

Wenn das Drucken immer noch nicht funktioniert, überprüfen Sie als nächstes das CUPS-Framework. Der ctxcups-Dienst ist für die Druckerverwaltung und kommuniziert mit dem Linux CUPS-Framework. Dies ist ein Prozess pro Maschine und kann mit folgendem Befehl überprüft werden:

```
service ctxcups status
```

Wenn der Dienst nicht ausgeführt wird, starten Sie ihn manuell:

```
service ctxcups start
```

Eine fehlerhafte Ausgabe kann durch einen nicht kompatiblen Druckertreiber verursacht werden. Pro Benutzer ist eine Treiberkonfiguration verfügbar und kann durch das Bearbeiten der Konfigurationsdatei ~/.CtxlpProfile konfiguriert werden.

```
[DEFAULT_PRINTER]

printername=

model=
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

ppdpath=

drivertype=

Das Feld printername enthält den Namen des aktuellen Clientstandarddruckers. Dieser Wert ist schreibgeschützt und darf nicht bearbeitet werden.

> **Important**
>
> Nehmen Sie nicht gleichzeitig Eingaben in die Felder **ppdpath**, **model** und **drivertype** vor, da nur eines für den zugeordneten Drucker wirksam ist.

Wenn der universelle Druckertreiber mit dem Clientdrucker nicht kompatibel ist, kann das Modell des nativen Druckertreibers mit der Option model= konfiguriert werden. Der aktuelle Modellname des Druckers kann mit dem Befehl lpinfo gefunden werden.

lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

...

Das Modell kann dann passend für den Drucker festgelegt werden:

Model=xerox/ph3115.ppd.gz

Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, kann der ppd-Dateipfad für den nativen Druckertreiber konfiguriert werden. Der ppdpath-Wert ist der absolute Pfad der nativen Druckertreiberdatei.

Beispielsweise ist ein ppd-Treiber unter /home/tester/NATIVE_PRINTER_DRIVER.ppd vorhanden.

ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd

Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Diese können als Treibertyp konfiguriert werden, wenn kein nativer Druckertreiber verfügbar ist.

Beispiel: Der Standarddruckertreibertyp des Client ist PCL5.

drivertype=pcl5

> **Hinweis**
>
> Citrix Receiver für Mac und Citrix Receiver für Linux unterstützen nur PostScript-Drucker, daher sind die universellen Druckertreiber PCL5 und PCL6 nicht relevant. In dieser Situation muss ppdpath oder das Modell des nativen Druckertreibers auf einen Nicht-PostScript-Drucker festgelegt werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### CDM funktioniert nicht

Das CDM-Feature enthält einen Daemonprozess (ctxcdmd). Wenn beim CDM-Feature ein Fehler auftritt, starten Sie die Linux VDA-Maschine neu und überprüfen Sie, ob der Daemon richtig gestartet wurde:

```
Ps -lef | grep ctxcdmd
```

Die Dateibenennung im zugeordneten Laufwerk sollte den Benennungsregeln für VDA und Receiver entsprechen.

# Bekannte Probleme

### Zustand der Feststelltaste in Citrix Receiver für Android kann beim Sitzungsroaming umgekehrt werden

Der Zustand der Feststelltaste kann aufgehoben werden, wenn über eine vorhandene Verbindung Roaming zu Citrix Receiver für Android erfolgt. Verwenden Sie als Workaround die Umschalttaste auf der erweiterten Tastatur, um zwischen Groß- und Kleinbuchstaben zu wechseln.

### Tastenkombinationen mit der Alt-Taste funktionieren nicht immer, wenn Sie mit Citrix Receiver für Mac eine Verbindung zu einem Linux VDA herstellen

Citrix Receiver für Mac sendet standardmäßig für die linke und die rechte Alt-Taste den Befehl "Alt Gr". Sie können dies in den Citrix Receiver-Einstellungen ändern, die Ergebnisse sind jedoch je nach Anwendung unterschiedlich.

### Neuere X-Clientbibliotheken können Tastaturprobleme unter SuSE Linux Enterprise Desktop 11 verursachen

Neuere Versionen der xorg-x11-libX11-Pakete unter SuSE Linux Enterprise Desktop 11 haben u. U. Probleme beim Ändern der Tastaturzuordnung, was zu Problemen bei der Tastaturfunktionalität in einer HDX-Sitzung führen kann. Diese Situation kann auftreten, wenn die installierte Version der Pakete im Bereich 7.4-5.11.11.1 bis 7.4-5.11.15.1 liegt.

Führen Sie als Workaround ein Rollback auf die SP3-Version des xorg-x11-libX11-Pakets durch. Änderungen der Tastaturzuordnung funktionieren dann normal. Beispiel:

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm – i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

Führen Sie das Rollback aus, bevor ein Benutzer sich an der Maschine anmeldet. Wenn dies während einer aktiven Sitzung erfolgt, werden die Einstellungen nicht wirksam, bis der Benutzer sich das nächste Mal anmeldet.

Wenn Sie ein Upgrade von SP3 ausführen, können die oben angegebenen xorg-x11-libX11-Pakete mit der aktuell installierten Version verknüpft werden, sodass sie während des Upgrades nicht geändert werden. Führen Sie vor dem Upgrade folgende Prozesse aus und fahren Sie dann normal mit dem Upgrade fort:

```
zypper al xorg-x11-libX11
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
zypper al xorg-x11-libX11-32bit
```

### Beim Verwenden von Linux VDA mit einem Delivery Controller von XenDesktop-Version 7.1 können Sitzungsstarts lange dauern

Der langsame Start wird durch CGP-Einstellungen in der ICA-Datei verursacht, die vom XD 7.1 Delivery Controller erstellt wurde. Wenn diese Einstellungen vorhanden sind, versucht Citrix Receiver, eine Verbindung über TCP-Port 2598 herzustellen. Entsprechend den Standardfirewalleinstellungen auf einigen Linux-Distributionen, z. B. SLED 12, werden die TCP SYN-Pakete abgelegt, was zu einem Timeout und dem langen Sitzungsstart führt. Konfigurieren Sie als Workaround die Firewall auf dem Linux VDA so, dass das TCP SYN-Paket am Port 2598 abgelehnt wird. Dieses Problem wurde in neueren Versionen des Delivery Controllers behoben.

### Fehlschlagen der Registrierung, wenn der Linux VDA der Domäne wieder hinzugefügt wird

Wenn ein Linux VDA der Domäne wieder hinzugefügt und ein neuer Satz Kerberos-Schlüssel generiert wird, kann der Broker unter bestimmten Umständen keinen Sicherheitskontext mit dem VDA herstellen. Oft ist der Grund, dass der Broker ein veraltetes zwischengespeichertes VDA-Dienstticket verwendet, das auf dem vorherigen Kerberos-Schlüsselsatz basiert. Der VDA kann zwar eine Verbindung mit dem Broker herstellen, jedoch kann der Broker keinen Sicherheitskontext zum VDA herstellen. Normalerweise schlägt die VDA-Registrierung dann fehl.

Dieses Problem löst sich irgendwann von selber, wenn das VDA-Dienstticket abläuft und erneuert wird, jedoch haben Diensttickets oft eine lange Lebensdauer. Dies kann möglicherweise viel zu lange dauern.

Sie lösen das Problem, indem Sie den Ticketcache des Brokers leeren. Starten Sie den Broker neu oder führen Sie als Administrator auf dem Broker folgenden Befehl an einer Eingabeaufforderung aus:

```
klist -li 0x3e4 purge
```

Damit werden alle Diensttickets im LSA-Cache des Netzwerkdienstprinzipals gelöscht, unter dem der Citrix Brokerdienst ausgeführt wird. Es werden jedoch auch Diensttickets für andere VDAs und möglicherweise andere Dienste entfernt. Dies ist aber kein Problem, die Diensttickets werden bei Bedarf einfach erneut vom KDC geladen.

### Plug-n-Play von Audio wird nicht unterstützt

Audioaufnahmegeräte sollten mit der Clientmaschine verbunden sein, bevor Sie mit dem Aufzeichnen von Audio in der ICA-Sitzung beginnen. Wenn ein Gerät angeschlossen wird, nachdem die Audioaufzeichnungsanwendung gestartet wurde, reagiert die Anwendung u. U. nicht mehr. Wenn dieses Problem auftritt, starten Sie die Anwendung neu. Ein ähnliches Problem kann auftreten, wenn Sie ein Aufzeichnungsgerät während der Aufzeichnung entfernen.

### Audiostörungen

Bei Windows 10 Receiver können während der Aufzeichnung Audiostörungen auftreten.

### CTXPS-Treiber ist mit einigen PLC-Druckern nicht kompatibel

Wenn Sie Druckausgabestörungen bemerken, legen Sie als Druckertreiber den nativen Druckertreiber des Herstellers fest.

### Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Clientdrucker drucken, wird die zu druckende Datei über die Serververbindung übertragen. Bei langsamen Verbindungen kann dies sehr lange dauern.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen werden angezeigt

Linux hat nicht das gleiche Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Durch Ändern der CUPS-Konfigurationsdatei /etc/cups/cupsd.conf kann der Administrator diese Benachrichtigungen deaktivieren.

Suchen Sie den aktuellen, in der Datei konfigurierten Richtliniennamen:

```
DefaultPolicy default
```

Wenn der Richtlinienname "default ist, fügen Sie die folgenden Zeilen im XML-Block der Standardrichtlinie hinzu.

```
# Job/subscription privacy...
JobPrivateAccess default
JobPrivateValues default
SubscriptionPrivateAccess default
SubscriptionPrivateValues default
... ...
    Require user @OWNER
    Order deny,allow


    Order deny,allow
```

# Glossar

Broker: XenDesktop-Komponente, die für die Vermittlung von HDX-Sitzungen auf den verschiedenen VDAs in einer XenDesktop-Bereitstellung verantwortlich ist. Er wird auch als DDC oder XenDesktop Controller bezeichnet.

Broker Agent: Komponente auf der Linux VDA-Maschine, die den Desktop bereitstellt. Der Broker Agent kommuniziert mit dem Broker und ermöglicht die Vermittlung von Sitzungen. Er besteht aus zwei Hauptkomponenten: dem VDA-Dienst und dem HDX-Dienst.

Citrix Director: Citrix Helpdesk-/Supportkonsole zum Überwachen und Steuern von XenDesktop-VDAs.

Citrix Studio: Citrix Verwaltungskonsole zum Konfigurieren von XenDesktop.

DDC: XenDesktop Desktop Delivery Controller. Wird auch als Broker oder Delivery Controller bezeichnet.

FQDN: Vollqualifizierter Domänenname (Fully Qualified Domain Name)

HDX: High Definition Experience-Protokoll. Wurde früher als Citrix ICA-Protokoll bezeichnet.

HDX-Dienst: Der Linux-Dienst (ctxhdx), der mit dem HDX-Protokoll eine Remoteverbindung zum virtuellen Linux-Desktop herstellt. Er kommuniziert mit dem VDA-Dienst zum Vermitteln von Sitzungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

RHEL: Red Hat Enterprise Linux. Eine kommerzielle Linux-Distribution von Red Hat.

SLED: SUSE Linux Enterprise Desktop. Eine kommerzielle Linux-Distribution von Novell.

SLES: SUSE Linux Enterprise Server. Eine kommerzielle Linux-Distribution von Novell.

VDA: Virtual Delivery Agent.

VDA-Dienst: Der Linux-Dienst (ctxvda), der mit dem Broker kommuniziert, um das Vermitteln von Sitzungen zu ermöglichen. Zudem kommuniziert er mit dem HDX-Dienst für die Bereitstellung von Remotesitzungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen einer Site

Aug 17, 2016

Unter der *Site* versteht man die XenApp- bzw XenDesktop-Bereitstellung. Sie umfasst die Delivery Controller und andere Kernkomponenten, Virtual Delivery Agents (VDAs), Verbindungen mit Hosts (falls verwendet) sowie die Maschinenkataloge und Bereitstellungsgruppen, die Sie erstellen und verwalten. Sie erstellen die Site nach der Installation der Kernkomponenten und bevor Sie den ersten Maschinenkatalog und die erste Bereitstellungsgruppe erstellen.

Beim Erstellen einer Site werden Sie automatisch für das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) registriert. Im Rahmen des CEIP werden anonyme Statistiken und Nutzungsinformationen gesammelt und an Citrix gesendet. Das erste Datenpaket wird rund sieben Tage nach dem Erstellen der Site an Citrix gesendet. Sie können Ihre Registrierung nach der Siteerstellung jederzeit ändern. Wählen Sie hierfür im Studio-Navigationsbereich **Konfiguration**, anschließend die Registerkarte "Produktsupport" und folgen Sie den Anweisungen. Informationen zum CEIP finden Sie unter http://more.citrix.com/XD-CEIP.

Der Benutzer, der eine Site erstellt, ist Volladministrator dieser Site. Weitere Informationen finden Sie im Artikel Delegierte Administration.

Lesen Sie diesen Artikel über die vor der Siteerstellung zu treffenden Vorbereitungen und Entscheidungen, bevor Sie den Assistenten für die Siteerstellung starten.

### Erstellen einer Site

Öffnen Sie Studio, falls es nicht geöffnet ist. Sie werden automatisch zu der Aktion zum Starten des Assistenten für die Siteerstellung geführt. Die Seiten des Assistenten decken folgende Elemente der Konfiguration ab:

Es stehen zwei Sitetypen zur Auswahl:

- **Anwendungs- und Desktopbereitstellungssite**: Wenn Sie eine Anwendungs- und Desktopbereitstellungssite erstellen, haben Sie die Wahl zwischen einer vollständigen Bereitstellung (empfohlen) oder einer leeren Site. Leere Sites sind nur teilweise konfiguriert und werden normalerweise von erfahrenen Administratoren erstellt.
- **Remote-PC-Zugriff-Site**: Sites dieses Typs ermöglichen Benutzern den Remotezugriff auf ihre Büro-PCs über eine sichere Verbindung.

Wenn Sie zu diesem Zeitpunkt eine Bereitstellung für die Anwendungs- und Desktopbereitstellung erstellen, können Sie eine Remote-PC-Zugriff-Bereitstellung später hinzufügen. Ebenso können Sie einer Remote-PC-Zugriff-Bereitstellung später eine vollständige Bereitstellung hinzufügen.

Geben Sie einen Namen für die Site ein. Nachdem die Site erstellt wurde, wird der Name oben im Studio-Navigationsbereich angezeigt: **Citrix Studio** (*Sitename*).

Die Seite **Datenbanken** enthält Einstellungen zur Einrichtung der Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank. Informationen zu Anforderungen für die Datenbanken und zu deren Einrichtung finden Sie im Artikel Datenbanken.

Wenn Sie bei der Siteerstellung die Installation der SQL Server Express-Datenbank zur Verwendung als Sitedatenbank


© 1999-2017 Citrix Systems, Inc. All rights reserved.

auswählen (= Standardeinstellung), erfolgt nach Installation der Datenbanksoftware ein Neustart. Der Neustart erfolgt nicht, wenn Sie die Installation der SQL Server Express-Datenbank zur Verwendung als Sitedatenbank nicht auswählen.

Wenn Sie keine standardmäßige SQL Server Express-Installation verwenden möchten, installieren Sie vor Erstellen der Site SQL Server auf den Maschinen. Die unterstützten Versionen werden im Artikel "Systemanforderungen" aufgeführt.

Wenn Sie bereits die Controller-Software auf anderen Servern installiert haben und der Site weitere Delivery Controller hinzufügen möchten, können Sie dies über diese Seite im Assistenten für die Siteerstellung tun. Wenn Sie Skripts für die Einrichtung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.

Überlegen Sie, ob Sie vorhandene Lizenzen verwenden möchten oder das 30-tägige kostenlose Probeabo, bei dem die Lizenzdateien später hinzugefügt werden können. Sie können Lizenzdateien auch über den Assistenten für die Siteerstellung hinzufügen oder herunterladen. Weitere Informationen finden Sie in der Dokumentation zur Lizenzierung.

Geben Sie die Adresse des Lizenzservers im Format *Name*:[*Port*] an. Der Name muss ein vollqualifizierter Domänenname (FQDN), ein NetBIOS-Name oder eine IP-Adresse sein, empfohlen wird die Verwendung eines FQDN. Wenn Sie die Portnummer auslassen, ist der Standardport 27000. Klicken Sie auf **Connect**. Sie können erst mit der nächsten Seite des Assistenten fortfahren, wenn eine Verbindung zum Lizenzserver hergestellt wurde.

Informationen finden Sie im Abschnitt Remote-PC-Zugriff unten.

Wenn Sie für die Bereitstellung von Anwendungen und Desktops VMs auf einem Host (Hypervisor oder Clouddienst) verwenden möchten, können Sie im Rahmen der Siteerstellung optional die erste Verbindung mit dem Host konfigurieren. Sie können außerdem Speicher- und Netzwerksressourcen für die Verbindung festlegen. Zu einem späteren Zeitpunkt können Sie die Verbindung und die Ressourcen modifizieren und/oder zusätzliche Verbindungen erstellen.

**Wichtig**: Konsultieren Sie bei der Konfiguration von Verbindung und Ressourcen über den Assistenten für die Siteerstellung den Artikel Verbindungen und Ressourcen:

- Abschnitt Informationsquellen für Verbindungstypen enthält Angaben zu Informationsquellen für die einzelnen unterstützten Verbindungstypen.
- Unter Hostspeicher werden die Speichertypen und Speicherverwaltungsmethoden beschrieben.
- In den Abschnitten Speicherverwaltung und Speicherauswahl wird erläutert, wie beim Erstellen einer Verbindung Speicherinformationen konfiguriert werden.

Wenn Sie zum Bereitstellen von Anwendungen und Desktops keine VMs auf einem Hypervisor oder in einem Clouddienst verwenden oder Studio für die Verwaltung von auf dedizierten Blade-PCs gehosteten Benutzerdesktops verwenden, wählen Sie als Verbindungstyp **Keine**.

Wenn Sie eine Remote-PC-Zugriff-Site konfigurieren und Wake-On-LAN verwenden möchten, wählen Sie als Hosttyp **Microsoft System Center Configuration Manager**.

Geben Sie auf der Seite **Verbindung** außerdem an, ob Sie Citrix Tools (z. B. Maschinenerstellungsdienste) oder andere Tools zum Erstellen von VMs auf dem Host verwenden möchten.

Konfigurieren Sie auf den Seiten **Speicher** und **Netzwerk** die angeforderten Informationen anhand der Anweisungen aus

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

den oben verlinkten Informationsquellen.

**Erinnerung**: Der Artikel Verbindungen und Ressourcen enthält detaillierte Anweisungen.

Sie können weitere Features zum Anpassen der Site auswählen. Wenn Sie das Kontrollkästchen eines Elements aktivieren, wird ein Dialogfeld zur Konfiguration angezeigt.

**AppDNA-Integration**

Wenn Sie AppDisks verwenden möchten und AppDNA installiert haben, können Sie mit diesem Feature Anwendungen auf AppDisks analysieren und Kompatibilitätsprobleme suchen und lösen. Weitere Informationen finden Sie im Artikel AppDisks.

**App-V-Veröffentlichung**

Aktivieren Sie dieses Feature, wenn Sie Anwendungen aus Microsoft App-V-Paketen auf App-V-Servern verwenden. Wenn Sie dieses Kontrollkästchen aktivieren, werden Sie zur Eingabe der URL des App-V-Verwaltungsservers und von URL und Portnummer des App-V- Veröffentlichungsservers aufgefordert.

Wenn Sie nur Anwendungen von App-V-Paketen in Netzwerkfreigaben verwenden, brauchen Sie das Feature nicht auszuwählen.

Sie können das Feature auch später in Studio aktivieren, deaktivieren und konfigurieren. Weitere Informationen finden Sie im Artikel App-V.

Informationen über Remote-PC-Zugriffsbereitstellungen finden Sie im Artikel Remote-PC-Zugriff.

Wenn Sie das Wake-On-LAN-Feature verwenden, führen Sie vor dem Erstellen der Site die entsprechende Konfiguration in Microsoft System Center Configuration Manager durch. Weitere Informationen finden Sie in dem Artikel zu Microsoft System Center Configuration Manager.

Für das Erstellen einer Remote-PC-Zugriff-Site gilt Folgendes:

- Wenn Sie Wake-On-LAN verwenden, geben Sie die Adresse, Anmeldeinformationen und Verbindungsinformationen für Microsoft System Center Configuration Manager auf der Seite **Energieverwaltung** an.
- Geben Sie Benutzer bzw. Benutzergruppen auf der Seite "Benutzer" an, denn es gibt keine Standardaktion zum automatischen Hinzufügen aller Benutzer. Geben Sie außerdem Maschinenkonten (Domänen- oder OU-Konten) auf der Seite **Maschinenkonten** des Assistenten an.

  Zum Hinzufügen von Benutzerinformationen klicken Sie auf **Benutzer hinzufügen**. Wählen Sie Benutzer und Benutzergruppen aus und klicken Sie dann auf **Benutzer hinzufügen**.

  Zum Hinzufügen von Maschinenkonten klicken Sie auf **Maschinenkonten hinzufügen**. Wählen Sie die Maschinenkonten aus und klicken Sie dann auf **Maschinenkonten hinzufügen**. Klicken Sie auf **Organisationseinheiten hinzufügen**. Wählen Sie die Domäne und die Organisationseinheiten und geben Sie an, ob Elemente in Unterordnern eingeschlossen werden. Klicken Sie auf **Organisationseinheiten hinzufügen**.

**Hinweis:** Beim Erstellen einer Remote-PC-Zugriff-Site wird automatisch ein Maschinenkatalog erstellt, der alle Maschinenkonten, die Sie über den Assistenten für die Siteerstellung hinzugefügt haben, enthält. Es wird automatisch eine

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Bereitstellungsgruppe mit allen von Ihnen hinzugefügten Benutzern und Gruppen erstellt.

Auf der letzten Seite des Assistenten für die Siteerstellung wird eine Zusammenfassung der von Ihnen angegebenen Informationen angezeigt. Verwenden Sie die Schaltfläche **Zurück**, wenn Sie etwas ändern möchten. Wenn Sie fertig sind, klicken Sie auf **Erstellen**, um die Siteerstellung zu starten.

# Testen einer Sitekonfiguration

Zum Durchführen der Tests nach der Siteerstellung wählen Sie oben im Navigationsbereich **Citrix Studio (Site** *Sitename***)** und klicken Sie dann in der Mitte auf **Site testen**. Sie können einen HTML-Bericht des Testergebnisses anzeigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen von Maschinenkatalogen

Aug 17, 2016

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem so genannten *Maschinenkatalog* verwaltet. Alle Maschinen in einem Maschinenkatalog haben den gleichen Betriebssystemtyp: Server oder Desktop. Ein Katalog mit Serverbetriebssystemmaschinen kann entweder Windows- oder Linux-Maschinen enthalten, nicht aber beides.

Nach dem Erstellen der Site werden Sie von Studio zur Erstellung des ersten Maschinenkatalogs geführt. Nach dem Erstellen des ersten Maschinenkatalogs werden Sie von Studio zur Erstellung der ersten Bereitstellungsgruppe geführt. Später können Sie den erstellten Katalog ändern und weitere Kataloge erstellen.

# Übersicht

Wenn Sie einen Maschinenkatalog für VMs erstellen, geben Sie an, wie diese bereitgestellt werden. Sie können die von Studio unterstützten Tools (z. B. Maschinenerstellungsdienste oder Provisioning Services) oder eigene Tools verwenden. Selbst wenn Sie die Maschinen bereits haben, d. h. keine Masterimages verwenden müssen, erstellen Sie mindestens einen Maschinenkatalog.

- Wenn Sie Maschinen mit Provisioning Services erstellen, lesen Sie die Dokumentation zu Provisioning Services.
- Bei Verwendung von Maschinenerstellungsdiensten (MCS) stellen Sie ein Masterimage (bzw. einen Snapshot) zum Erstellen identischer virtueller Maschinen im Katalog bereit. Vor dem Erstellen des Katalogs verwenden Sie Tools auf dem Hypervisor bzw. im Clouddienst zum Erstellen und Konfigurieren des Masterimages. Dazu gehört auch die Installation eines Virtual Delivery Agents (VDA) auf dem Image. Beim anschließenden Erstellen des Maschinenkatalogs in Studio wählen Sie das Image (bzw. dessen Snapshot) und geben die Anzahl der in dem Katalog zu erstellenden VMs und weitere Informationen an.

Beim Erstellen des ersten Maschinenkatalogs mit MCS oder PVS verwenden Sie die Hostverbindung, die Sie beim Erstellen der Site konfiguriert haben. Nach dem Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe können Sie die Informationen über diese Verbindung ändern und zusätzliche Verbindungen erstellen.

Nach Abschließen des Assistenten zum Erstellen von Maschinenkatalogen werden automatisch Tests ausgeführt, um sicherzustellen, dass der Katalog richtig konfiguriert wurde. Wenn die Tests abgeschlossen sind, können Sie einen Testbericht anzeigen. Sie können diese Tests bei Bedarf später über **Citrix Studio** *Sitename* im Studio-Navigationsbereich ausführen.

**Tipp:** Wenn Sie einen Katalog direkt mit dem PowerShell-SDK anstelle von Studio erstellen, können Sie alternativ zu einem Image bzw. einem Image-Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

Für Windows XP- und Windows Vista-Maschinen muss eine ältere VDA-Version verwendet werden. Die Verwendung der neuesten Produktfeatures ist hier nicht möglich. Wenn Sie diese Maschinen nicht auf eine unterstützte Windows-Betriebssystemversion aktualisieren können, empfiehlt Citrix, sie in einem separaten Maschinenkatalog zu führen.

Nachdem Sie Informationen im Assistenten zum Erstellen von Maschinenkatalogen eingegeben haben, erfolgen die nachfolgend aufgeführten Aktionen in MCS.

- Wenn Sie im Assistenten ein Masterimage anstelle eines Snapshots ausgewählt haben, erstellt MCS einen Snapshot.
- MCS erstellt eine vollständige Kopie des Snapshots und fügt diese an jedem in der Hostverbindung definierten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Speicherort hinzu.
- MCS fügt Active Directory Desktops hinzu, wodurch eindeutige Identitäten erstellt werden.
- MCS erstellt die im Assistenten angegebene Anzahl VMs mit jeweils zwei Datenträgern. Neben den beiden Datenträgern wird jeweils ein Master am gleichen Speicherort gespeichert. Wenn Sie mehrere Speicherorte definiert haben, werden an jedem die folgenden Datenträgertypen erstellt:
  - Vollständige Kopie des Snapshots (siehe oben); diese ist schreibgeschützt und wird von allen gerade erstellten VMs gemeinsam genutzt.
  - Eine eindeutige 16-MB-Identitätsdisk, durch die jede VM eine eindeutige Identität erhält. Jede VM erhält eine Identitätsdisk.
  - Ein eindeutiger differenzierender Datenträger zum Speichern der auf der VM erfolgten Schreibvorgänge. Dieser Datenträger ist, sofern dies vom Hostspeicher unterstützt wird, für schlanke Speicherzuweisung geeignet und kann bei Bedarf auf die maximale Größe des Masterimages, anwachsen. Jede VM erhält einen differenzierenden Datenträger. Auf diesem Datenträger werden Änderungen, die während der Sitzungen gemacht werden, gespeichert. Er ist für dedizierte Desktops permanent und für gepoolte Desktops flüchtig, d. h. er wird bei jedem Neustart gelöscht und neu erstellt.

# Vorbereiten eines Masterimages auf dem Hypervisor bzw. im Clouddienst

**Tipp:** Informationen über das Erstellen von Verbindungen mit Hypervisors und Cloudanbietern finden Sie im Artikel Verbindungen und Ressourcen.

Das Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software.

Gut zu wissen:

- Masterimages werden ggf. auch als Klonimage, Golden Image, Basis-VM oder Basisimage bezeichnet. Hosthersteller und Clouddienstanbieter verwenden andere Bezeichnungen.
- Wenn Sie Provisioning Services verwenden, können Sie entweder ein Masterimage oder einen physischen Computer als Masterzielgerät verwenden. In Provisioning Services wird für Images eine andere Terminologie verwendet als in MCS (Einzelheiten s. zugehörige Dokumentation).
- Stellen Sie sicher, dass Ihr Host genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der Maschinen hat, die Sie erstellen möchten.
- Konfigurieren Sie den für Desktops und Anwendungen erforderlichen Speicherplatz auf der Festplatte, da dieser Wert später nicht im Maschinenkatalog geändert werden kann.
- Bei Remote-PC-Zugriff-Maschinenkatalogen werden keine Masterimages verwendet.
- Hinweise zur Microsoft Key Management Server-Aktivierung bei Verwendung der Maschinenerstellungsdienste: Wenn Ihre Bereitstellung 7.x-VDAs mit einem XenServer 6.1- oder 6.2-Host, einem vSphere-Host oder einem Microsoft System Center Virtual Machine Manager-Host enthält, müssen Sie Microsoft Windows oder Microsoft Office nicht manuell zurücksetzen. Wenn die Bereitstellung einen 5.x-VDA mit einem XenServer 6.0.2-Host enthält, lesen Sie CTX128580.
- Installieren und konfigurieren Sie die folgende Software auf dem Masterimage:
  - Integrationstools für den Hypervisor (z. B. XenServer-Tools, Hyper-V-Integrationsdienste oder VMware-Tools). Wenn Sie diesen Schritt auslassen, funktionieren die Anwendungen und Desktops unter Umständen nicht richtig.
  - Einen VDA – Citrix empfiehlt die Installation der neuesten Version, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl.
  - Tools von Drittanbietern, zum Beispiel Antivirensoftware oder Agents zur elektronischen Softwareverteilung.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Konfigurieren Sie Dienste mit den für Benutzer und Maschinentyp geeigneten Einstellungen (z. B. Featureupdates).

- Anwendungen von Drittanbietern, die Sie nicht virtualisieren möchten. Citrix empfiehlt das Virtualisieren von Anwendungen, da dies die Kosten erheblich senkt, denn das Masterimage muss nach dem Hinzufügen oder Neukonfigurieren einer Anwendung nicht aktualisiert werden. Außerdem belegen weniger installierte Anwendungen weniger Platz auf Masterimage-Festplatten, wodurch Speicherkosten eingespart werden.
- App-V-Clients mit den empfohlenen Einstellungen, wenn Sie App-V-Anwendungen veröffentlichen möchten. Der App-V-Client ist bei Microsoft erhältlich.
- Wenn Sie MCS verwenden und Microsoft Windows in lokalisierter Version ausführen möchten, installieren Sie die Gebietsschemas und Sprachpakete. Wenn ein Snapshot beim Provisioning erstellt wird, verwenden die bereitgestellten VMs die installierten Gebietsschemas und Sprachpakete.

**Wichtig:** Wenn Sie Provisioning Services oder MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.

Vorbereiten eines Masterimages

1. Erstellen Sie mit dem Verwaltungstool des Hypervisors ein neues Masterimage und installieren Sie dann das Betriebssystem sowie alle Service Packs und Updates Geben Sie die Anzahl der vCPUs an. (Sie können diesen Wert auch angeben, wenn Sie den Maschinenkatalog erstellen, aber nur, wenn Sie PowerShell verwenden. Sie können die Anzahl der vCPUs nicht beim Erstellen eines Katalogs in der Studio-Benutzeroberfläche angeben.) Konfigurieren Sie jedoch den für Desktops und Anwendungen erforderlichen Speicherplatz auf der Festplatte, da dieser Wert später nicht im Katalog geändert werden kann.
2. Stellen Sie sicher, dass die Festplatte am Gerätestandort 0 verbunden ist. Dieser Standort ist in den meisten Standardmasterimagevorlagen automatisch konfiguriert; in einigen benutzerdefinierten Vorlagen ist dies jedoch nicht unbedingt der Fall.
3. Installieren und konfigurieren Sie die oben aufgeführte Software auf dem Masterimage:
4. Bei Verwendung von Provisioning Services erstellen Sie eine VHD-Datei für die vDisk von Ihrem Masterzielgerät, bevor Sie das Masterzielgerät in eine Domäne einbinden. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
5. Fügen Sie das Masterimage der Domäne hinzu, der Desktops und Anwendungen angehören werden, und stellen Sie sicher, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden. Das Masterimage muss keiner Domäne angefügt werden, wenn Sie MCS verwenden. Die bereitgestellten Maschinen werden Mitglied der im Assistenten zum Erstellen von Maschinenkatalogen angegebenen Domäne.
6. Citrix empfiehlt, dass Sie einen Snapshot des Masterimages erstellen und benennen, damit es künftig identifiziert werden kann. Wenn Sie ein Masterimage anstelle eines Snapshots beim Erstellen eines Maschinenkatalogs angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Wenn Sie für Ihre Hostinginfrastruktur XenServer verwenden, benötigen GPU-fähige Maschinen ein dediziertes Masterimage. Diese VMs erfordern Videotreiber, die GPUs unterstützen und so konfiguriert sind, dass die VMs Software verwenden können, die den GPU für Vorgänge verwendet.

1. Erstellen Sie in XenCenter eine VM mit Standard-VGA sowie Netzwerken und einer vCPU.
2. Aktualisieren Sie die VM-Konfiguration so, dass der GPU (entweder Passthrough oder vGPU) verwendet werden kann.
3. Installieren Sie ein unterstütztes Betriebssystem und aktivieren Sie RDP.
4. Installieren Sie XenServer-Tools und NVIDIA-Treiber.
5. Deaktivieren Sie die VNC-Verwaltungskonsole (Virtual Network Computing), um die Leistung zu optimieren, und starten Sie anschließend die VM neu.
6. Sie werden aufgefordert, RDP zu verwenden. Installieren Sie mit RDP den VDA und starten Sie dann die VM neu.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

7. Optional können Sie einen Snapshot der VM erstellen und als Vorlage für andere GPU-Masterimages verwenden.
8. Installieren Sie mit RDP kundenspezifische Anwendungen, die in XenCenter konfiguriert werden und GPU-Funktionen verwenden.

# Erstellen eines Maschinenkatalogs mit Studio

Bevor Sie den Assistenten zum Erstellen von Maschinenkatalogen starten, lesen Sie diesen Abschnitt, damit Sie wissen, welche Optionen Sie auswählen und welche Informationen Sie angeben müssen. Je nach den von Ihnen ausgewählten Optionen werden einige der unten beschriebenen Seiten möglicherweise nicht angezeigt oder heißen anders.

**Wichtig:** Wenn Sie ein Masterimage verwenden, vergewissern Sie sich vor dem Erstellen des Maschinenkatalogs, dass auf dem Image ein VDA installiert ist.

In Studio:

- Wenn Sie eine Site, jedoch noch keinen Maschinenkatalog erstellt haben, führt Studio Sie zum richtigen Startpunkt zur Erstellung eines Maschinenkatalogs.
- Wenn Sie bereits einen Maschinenkatalog erstellt haben und einen weiteren erstellen möchten, wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** und dann im Aktionsbereich **Maschinenkatalog erstellen**.

Der Assistent führt Sie durch die nachfolgend beschriebenen Einstellungen. Die angezeigten Assistentenseiten können sich je nach der von Ihnen vorgenommenen Auswahl unterscheiden.

Jeder Katalog enthält nur Maschinen eines Typs:

- **Serverbetriebssystem:** Ein Maschinenkatalog für Serverbetriebssysteme bietet Desktops und Anwendungen, die von mehreren Benutzern verwendet werden können. Auf den Maschinen können die unterstützten Versionen von Windows oder Linux ausgeführt werden, ein Katalog kann jedoch nur Windows- oder Linux-Maschinen enthalten.
- **Desktopbetriebssystem:** Ein Maschinenkatalog für Desktopbetriebssysteme bietet Desktops und Anwendungen, die unterschiedlichen Benutzern zugewiesen werden.
- **Remote-PC-Zugriff:** Ein Remote-PC-Zugriff-Katalog bietet Benutzern Remotezugriff auf ihre physischen Büro-Desktopmaschinen. Bei Remote-PC-Zugriff wird VPN nicht für die Sicherheit benötigt.

Auf der Seite **Maschinenverwaltung** wird angegeben, wie die Maschinen verwaltet und mit welchem Tool sie bereitgestellt werden.

Wählen Sie, ob für Maschinen in dem Katalog die Energieverwaltung über Studio ausgeführt werden soll.

- Maschinen mit Energieverwaltung über Studio oder über eine Cloudumgebung bereitgestellte Maschinen (z. B. VM oder Blade-PC). Diese Option ist nur verfügbar, wenn bereits eine Hypervisor- oder Clouddienstverbindung konfiguriert wurde.
- Maschinen ohne Energieverwaltung (z. B. physische Maschinen).

Wenn Sie angegeben haben, dass die Energieverwaltung der Maschinen über Studio oder die Maschinenbereitstellung über eine Cloudumgebung erfolgen soll, wählen Sie aus, welches Tool Sie für die Maschinenbereitstellung verwenden möchten.

- **Maschinenerstellungsdienste (MCS):** verwendet ein Masterimage zum Erstellen und Verwalten virtueller Maschinen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bei Maschinenkatalogen in Cloudumgebungen wird MCS verwendet. MCS ist für physische Maschinen nicht verfügbar.

- **Provisioning Services:** verwaltet Zielgeräte als Gerätesammlung. Eine als Image eines Masterzielgeräts erstellte Provisioning Services-vDisk liefert Desktops und Anwendungen. Diese Option ist für Cloudbereitstellungen nicht verfügbar.
- **Anderes:** Tool, mit dem bereits Maschinen im Datencenter verwaltet werden. Citrix empfiehlt die Verwendung von Microsoft System Center Configuration Manager oder einer anderen Drittanbieteranwendung, um sicherzustellen, dass die Maschinen in dem Katalog konsistent sind.

Über die Seite **Desktoperfahrung** wird der Typ der zu erstellenden Desktops festgelegt. Die Seite wird nur angezeigt, wenn ein Katalog für Desktopbetriebssystemmaschinen erstellt wird. Der Typ hängt davon ab, ob die jeweilige Maschine einem Benutzer zugewiesen ist und was mit den Änderungen des Benutzers passiert, wenn die Maschine neu gestartet wird.

Es gibt drei Typen:

- **Gepoolt, zufällig:** Desktops werden nach dem Zufallsprinzip zugewiesen, die Benutzer werden bei jeder Anmeldung mit einem neuen Desktop verbunden. Wenn ein Benutzer sich abmeldet, wird der Desktop für einen anderen Benutzern verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen verworfen.
- **Gepoolt, statisch:** Desktops werden bleiben zugewiesen, die Benutzer werden bei jeder Anmeldung mit dem gleichen Desktop verbunden. Wenn ein Benutzer sich abmeldet, bleibt der Desktop nur für diesen Benutzer verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen verworfen.
- **Dediziert:** Desktops sind dauerhaft einem Benutzer zugewiesen. Wenn ein Benutzer sich abmeldet, bleibt der Desktop nur für diesen Benutzer verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen beibehalten. Änderungen können auf einem lokalen VM-Datenträger oder in einem Laufwerk auf einer eigenen persönlichen vDisk gespeichert werden.

Wählen Sie die Verbindung mit dem Host-Hypervisor oder Clouddienst und anschließend den zuvor erstellten Snapshot bzw. die zuvor erstellte virtuelle Maschine. Beim Erstellen des ersten Maschinenkatalogs ist nur die Verbindung verfügbar, die Sie beim Erstellen der Site konfiguriert haben.

Erinnerung:

- Wenn Sie Provisioning Services oder MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.
- Wenn Sie ein Masterimage anstelle eines Snapshots angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Vergewissern Sie sich, dass auf dem Masterimage die aktuelle VDA-Version installiert ist, damit Sie die neuesten Produktfeatures verwenden können. Behalten Sie die Standardeinstellung für **Wählen Sie die VDA-Version** auf der Seite des Assistenten bei.

Eine Fehlermeldung wird angezeigt, wenn Sie einen Snapshot oder eine VM auswählen, der bzw. die nicht mit dem zuvor im Assistenten ausgewählten Tool zur Maschinenverwaltung kompatibel ist.

Wählen Sie mindestens eine Sicherheitsgruppe für die virtuellen Maschinen. Diese werden nur angezeigt, wenn die Verfügbarkeitszone Sicherheitsgruppen unterstützt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entscheiden Sie, ob die Maschinen Hardware gemeinsam oder dedizierte Hardware verwenden sollen.

Der Titel der Seite hängt von der Bereitstellungsmethode ab, die Sie auf der Seite **Maschinenverwaltung** gewählt haben.

- Wenn Sie MCS gewählt haben, lautet der Titel **Virtuelle Maschinen**.
- Wenn Sie Provisioning Services gewählt haben, lautet der Titel **Gerätesammlung**.
- Wenn Sie "Anderes" gewählt haben, lautet der Titel **VMs und Benutzer**.

Seite:

- Legen Sie fest, wie viele virtuelle Maschinen erstellt werden sollen.
- Wählen Sie die Menge Arbeitsspeicher in MB, die jede Maschine haben soll.
- Wenn Sie auf der Seite **Desktoperfahrung** festgelegt haben, dass die Änderungen der Benutzer an Desktops auf separaten Personal vDisks gespeichert werden sollen, geben Sie deren Größe in Gigabyte und den Laufwerksbuchstaben an.
- Wenn Ihre Bereitstellung mehrere Zonen enthält, können Sie eine Zone für den Katalog wählen.
- Wenn Sie Maschinen mit MCS bereitstellen und gepoolte zufällige VMs ohne persönliche vDisks erstellen, können Sie einen Cache für temporäre Daten auf jeder Maschine konfigurieren. Weitere Informationen finden Sie im nächsten Abschnitt.

**Wichtig:** Jede VM hat dann eine Festplatte. Deren Größe wird im Masterimage festgelegt. Sie können die Festplattengröße im Katalog nicht ändern.

## Konfigurieren eines Cache für temporäre Daten

Das lokale Zwischenspeichern temporärer Daten auf VMs ist optional. Sie können den temporären Datencache auf Maschinen aktivieren, wenn Sie MCS zum Verwalten gepoolter (nicht dedizierter) Maschinen in einem Katalog verwenden. Wenn für einen Katalog eine Verbindung verwendet wird, durch die die Speicherung temporärer Daten festgelegt ist, können Sie bei der Katalogerstellung den temporäre Datencache aktivieren und konfigurieren.

Zum Aktivieren der Zwischenspeicherung temporärer Daten muss der VDA auf jeder Maschine in dem ausgewählten Katalog mindestens in Version 7.9 vorliegen.

Beim Erstellen der Verbindung für den Katalog geben Sie an, ob die temporären Daten in einem freigegebenen oder dem lokalen Speicher abgelegt werden sollen. Einzelheiten hierzu finden Sie im Artikel Verbindungen und Ressourcen. Beim Aktivieren und Konfigurieren des temporären Cache in einem Katalog werden zwei Kontrollkästchen und Werte verwendet: **Dem Cache zugewiesener Speicher (MB)** und **Größe des Datenträgercache (GB)**. Die Standardwerte unterscheiden sich je nach Verbindungstyp. Die Standardwerte sind in den meisten Fällen ausreichen. Allerdings muss der für Folgendes erforderliche Speicherplatz berücksichtigt werden:

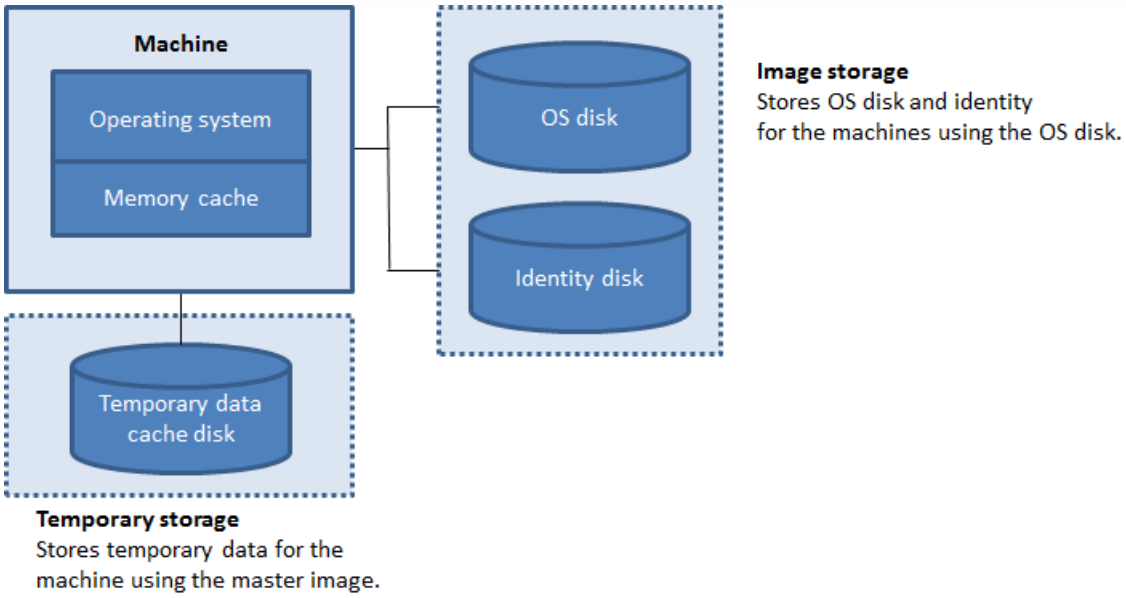
- Von Windows selbst erstellte temporäre Datendateien, einschließlich der Windows-Auslagerungsdatei
- Benutzerprofildaten
- ShareFile-Daten, die mit Benutzersitzungen synchronisiert werden
- Gegebenenfalls von einem Sitzungsbenutzer erstellte oder kopierte Daten und alle Anwendungen, die Benutzer möglicherweise sitzungsintern installieren

Windows gestattet nicht, dass für eine Sitzung deutlich mehr Cache verwendet wird, als es freien Speicherplatz auf dem ursprünglichen Masterimage gibt, über das die Maschinen des Maschinenkatalogs bereitgestellt werden. Es ergibt

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

beispielsweise keinen Sinn, eine Cachegröße von 20 GB festzulegen, wenn auf dem Masterimage nur 10 GB freier Speicherplatz verfügbar sind.

Wenn Sie das Kontrollkästchen **Größe des Datenträgercache** aktivieren, werden temporäre Daten zunächst in den Arbeitsspeichercache geschrieben. Sobald das über **Dem Cache zugewiesener Speicher** konfigurierte Limit erreicht ist, werden die ältesten Daten in den temporären Datenträgercache verschoben.




Der Arbeitsspeichercache ist Teil des auf jeder Maschine verfügbaren Arbeitsspeichers. Wenn Sie das Kontrollkästchen **Dem Cache zugewiesener Speicher** aktivieren, sollten Sie daher ggf. die Gesamtmenge des Arbeitsspeichers auf jeder Maschine erhöhen.

Wenn Sie das Kontrollkästchen **Dem Cache zugewiesener Speicher** deaktivieren und das Kontrollkästchen **Größe des Datenträgercache** aktiviert lassen, werden temporäre Daten unter minimaler Arbeitsspeichercachebelegung direkt in den Datenträgercache geschrieben.

Das Ändern der Größe des Datenträgercache kann die Leistung beeinträchtigen. Die Größe muss gemäß den Anforderungen der Benutzer und der Maschinenlast gewählt werden.

**Wichtig:** Wenn der Datenträgercache keinen Speicherplatz mehr aufweist, können die Benutzer ihre Sitzungen nicht fortsetzen.

Wenn Sie das Kontrollkästchen **Größe des Datenträgercache** deaktivieren, wird kein Datenträgercache erstellt. Geben Sie in diesem Fall für **Dem Cache zugewiesener Speicher** einen Wert ein, der für sämtliche temporären Daten ausreicht. Dies ist nur möglich, wenn große RAM-Volumen zur Zuweisung für jede VM verfügbar sind.

Wenn Sie beide Kontrollkästchen deaktivieren, werden temporäre Daten nicht zwischengespeichert, sondern für jede VM auf den differenzierenden Datenträger (im Betriebssystemspeicher) geschrieben. (Dies ist die Provisioning-Aktion in Releases vor 7.9.)

Die Zwischenspeicherung darf nicht aktiviert sein, wenn ein Katalog zum Erstellen von AppDisks verwendet werden soll.

Die Cachewerte für einen Maschinenkatalog können nach dessen Erstellung nicht geändert werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Sie mehrere Netzwerkkarten verwenden möchten, weisen Sie jeder ein virtuelles Netzwerk zu. Sie können beispielsweise einer Karte ein bestimmtes sicheres Netzwerk und einer anderen ein häufiger verwendetes Netzwerk zuweisen. Auf dieser Seite können Sie auch Netzwerkkarten hinzufügen und entfernen.

Geben Sie die hinzuzufügenden Active Directory-Maschinenkonten oder Organisationseinheiten an, die Benutzern oder Benutzergruppen entsprechen (dies gilt nur für Remote-PC-Zugriff-Kataloge). Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten.

Sie können eine zuvor konfigurierte Energieverwaltungsverbindung auswählen oder die Energieverwaltung nicht verwenden. Wenn Sie die Energieverwaltung verwenden möchten, jedoch noch keine geeignete Verbindung konfiguriert wurde, können Sie die Verbindung später erstellen und dann die Energieverwaltungseinstellungen des Maschinenkatalogs entsprechend bearbeiten.

Jede Maschine im Maschinenkatalog benötigt ein Active Directory-Computerkonto. Geben Sie an, ob neue Konten erstellt oder vorhandene Konten verwendet werden sollen, und geben Sie den Speicherort für diese Konten an.

- Wenn Sie neue Konten erstellen, müssen Sie Zugang zu einem Domänenadministratorkonto für die Domäne haben, in der die Maschinen residieren werden.

  Legen Sie für die zu erstellenden Maschinen das Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema "PC-Vertrieb-##" (und Aktivierung von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03" usw.

- Wenn Sie bestehende Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf "Importieren" und geben Sie eine CSV-Datei mit Kontonamen an. Die importierte Datei muss folgendes Format aufweisen:

  [ADComputerkonto]
  ADComputerkontoname.domäne

  ...

  Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Da diese Konten von Studio verwaltet werden, gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort (muss für alle Konten gleich sein) an.

Bei Katalogen mit physischen oder vorhandenen Maschinen wählen Sie vorhandene Konten aus oder importieren Sie diese, und weisen Sie jeder Maschine sowohl ein Active Directory-Computerkonto als auch ein Benutzerkonto zu.

Bei Maschinen, die mit Provisioning Services erstellt wurden, werden Computerkonten für Zielgeräte anders verwaltet. Weitere Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Überprüfen Sie auf der Seite **Zusammenfassung** Ihre Einstellungen. Geben Sie einen Namen und eine Beschreibung für den

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Katalog ein. Diese Informationen werden in Studio angezeigt.

Prüfen Sie die Informationen, die Sie angegeben haben, und klicken Sie auf **Fertig stellen**, um die Katalogerstellung zu starten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwalten von Maschinenkatalogen

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Hinzufügen von Maschinen im Maschinenkatalog
- Löschen von Maschinen aus einem Maschinenkatalog
- Ändern einer Maschinenkatalogbeschreibung oder der Remote-PC-Zugriff-Einstellungen
- Umbenennen von Maschinenkatalogen
- Verschieben eines Maschinenkatalogs in eine andere Zone
- Löschen eines Maschinenkatalogs
- Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog
- Aktualisieren von Maschinenkatalogen
- Aktualisieren eines Maschinenkatalogs


# Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen, entfernen und umbenennen, Maschinenbeschreibungen ändern und die Active Directory-Computerkonten des Katalogs verwalten.

Zur Verwaltung von Katalogen gehören ggf. auch die Aktualisierung des Betriebssystems und der Antivirensoftware der enthaltenen Maschinen, ein Upgrade des Betriebssystems und Änderungen an der Konfiguration.

- Maschinenkataloge mit gepoolt-zufälligen Maschinen, die mit Maschinenerstellungsdienste (MCS) erstellt wurden, können Sie pflegen, indem Sie das Masterimage des Katalogs und dann die Maschinen aktualisieren. So können Sie eine große Anzahl Maschinen effizient aktualisieren. Bei mit Provisioning Services erstellten Maschinen werden Updates über die vDisk verteilt. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
- Bei Katalogen mit statischen (permanent zugewiesenen) oder Remote-PC-Zugriff-Maschinen verwalten Sie Updates an den Maschinen der Benutzer Studio-extern entweder einzeln oder zusammen mit Bereitstellungssoftware von Drittanbietern.

Weitere Informationen zum Erstellen und Verwalten von Verbindungen mit Hosthypervisors und Clouddiensten finden Sie im Artikel Verbindungen und Ressourcen.

# Hinzufügen von Maschinen im Maschinenkatalog

Vorbereitungen:

- Stellen Sie sicher, dass der Virtualisierungshost (Hypervisor oder Clouddienstanbieter) genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der zusätzlichen Maschinen hat.
- Stellen Sie sicher, dass Sie genügend ungenutzte Active Directory-Computerkonten haben. Wenn Sie bestehende Konten verwenden, können Sie nur so viele Maschinen erstellen, wie Sie Konten haben.
- Wenn Sie Active Directory-Computerkonten für die zusätzlichen Maschinen mit Studio erstellen, müssen Sie die erforderlichen Domänenadministratorrechte haben.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Hinzufügen von Maschinen zum Maschinenkatalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Aktionsbereich **Maschinen hinzufügen**.
3. Legen Sie die Anzahl der hinzuzufügenden virtuellen Maschinen fest.
4. Gibt es nicht genügend Active Directory-Konten für die Zahl der VMs, die Sie hinzufügen möchten, wählen Sie die Domäne und den Speicherort, an dem Konten erstellt werden sollen. Legen Sie ein Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema "PC-Vertrieb-##" (und Aktivierung von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03" usw.
5. Wenn Sie bestehende Active Directory-Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf **Importieren** und geben Sie eine CSV-Datei mit Kontonamen an. Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Da diese Konten von Studio verwaltet werden, gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an. Dieses muss für alle Konten gleich sein.

Die Maschinen werden in einem Hintergrundprozess erstellt, der beim Erstellen einer großen Zahl von Maschinen lange dauern kann. Die Maschinenerstellung wird fortgesetzt, selbst wenn Sie Studio schließen.

# Löschen von Maschinen aus einem Maschinenkatalog

Wenn Sie eine Maschine aus einem Maschinenkatalog löschen, können Benutzer nicht mehr darauf zugreifen. Vergewissern Sie sich vor dem Löschen daher, dass folgende Bedingungen erfüllt sind:

- Die Benutzerdaten wurden gesichert oder werden nicht mehr benötigt.
- Alle Benutzer sind abgemeldet. Durch das Aktivieren des Wartungsmodus wird verhindert, dass neue Verbindungen mit einer Maschine hergestellt werden.
- Die Maschinen sind ausgeschaltet.

Löschen von Maschinen aus einem Maschinenkatalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** aus.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine oder mehrere Maschinen und dann im Aktionsbereich **Löschen**.

Wählen Sie aus, ob die Maschinen wirklich gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen.

# Ändern einer Maschinenkatalogbeschreibung oder der Remote-PC-Zugriff-Einstellungen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog bearbeiten**.
3. (Nur bei Remote-PC-Zugriff-Katalogen) Auf der Seite **Energieverwaltung** können Sie die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Energieverwaltungseinstellungen ändern und eine Energieverwaltungsverbindung auswählen. Verwenden Sie die Seite **Organisationseinheiten** zum Hinzufügen und Entfernen von Active Directory-Organisationseinheiten.

4. Ändern Sie auf der Seite **Beschreibung** die Beschreibung des Maschinenkatalogs.

# Umbenennen von Maschinenkatalogen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog umbenennen**.
3. Geben Sie den neuen Namen ein.

# Verschieben eines Maschinenkatalogs in eine andere Zone

Wenn eine Site mehrere Zonen enthält, können Sie Maschinenkataloge von Zone zu Zone verschieben.

**Vorsicht:** Wenn Sie einen Maschinenkatalog aus dem Hypervisor oder Clouddienst mit den zugehörigen VMs in eine andere Zone verschieben, kann sich dies negativ auf die Leistung auswirken.

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Verschieben**.
3. Wählen Sie die Zone aus, in die Sie den Katalog verschieben möchten.

# Löschen eines Maschinenkatalogs

Vor dem Löschen eines Maschinenkatalogs müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind abgemeldet und es werden keine getrennten Sitzungen ausgeführt.
- Der Wartungsmodus ist für alle Maschinen in dem Katalog aktiviert, damit keine neuen Verbindungen hergestellt werden können.
- Alle Maschinen in dem Katalog sind ausgeschaltet.
- Dem Katalog ist keine Bereitstellungsgruppe zugewiesen, d. h. keine Bereitstellungsgruppe enthält Maschinen aus dem Katalog.

Löschen eines Maschinenkatalogs

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog löschen**.
3. Geben Sie an, ob die Maschinen in dem Katalog gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Computerkonten beibehalten, deaktiviert oder gelöscht werden sollen.

# Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zum Verwalten von Active Directory-Konten in einem Maschinenkatalog haben Sie folgende Möglichkeiten:

- Freigeben nicht verwendeter Maschinenkonten durch Entfernen von Active Directory-Computerkonten aus Desktopbetriebssystem- und Serverbetriebssystemmaschinenkatalogen. Diese Konten können dann für andere Maschinen verwendet werden.
- Hinzufügen von Konten, damit beim Hinzufügen weiterer Maschinen zum Katalog Computerkonten bereit stehen. Verwenden Sie keinen Schrägstrich (/) im Namen von Organisationseinheiten.

Verwalten von Active Directory-Konten

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Aktionsbereich **Active Directory-Konten verwalten**.
3. Entscheiden Sie, ob Sie Computerkonten hinzufügen oder löschen möchten. Wenn Sie Konten hinzufügen, geben Sie an, wie mit den Kennwörtern verfahren werden soll: Setzen Sie entweder alle zurück oder geben Sie ein für alle Konten geltendes Kennwort ein. Sie können die Kennwörter zurückzusetzen, wenn Sie die aktuellen Kennwörter nicht kennen. Zum Zurücksetzen von Kennwörtern müssen Sie die entsprechende Berechtigung haben. Wenn Sie ein Kennwort eingeben, wird das Kennwort von Konten beim Importieren geändert. Wenn Sie ein Konto löschen, legen Sie fest, ob das Konto in Active Directory beibehalten, deaktiviert oder gelöscht werden soll.

**Hinweis:** Sie können auch angeben, ob Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen, wenn Sie Maschinen aus einem Katalog entfernen oder einen Katalog löschen.

# Aktualisieren von Maschinenkatalogen

Citrix empfiehlt, vor dem Durchführen von Updates von Maschinen in einem Katalog Kopien oder Snapshots der Masterimages zu speichern. In der Datenbank wird von jedem Masterimage eines Maschinenkatalogs ein historischer Datensatz beibehalten. Bei Problemen mit Updates, die auf den Benutzerdesktops bereitgestellt wurden, können Sie das Masterimage auf die vorherige Version zurücksetzen und die Downtime für Benutzer minimieren. Masterimages dürfen nicht gelöscht, verschoben oder umbenannt werden, da ansonsten Kataloge nicht auf ihre Verwendung zurückgesetzt werden können.

Bei Maschinenkatalogen, die Provisioning Services verwenden, müssen Sie eine neue vDisk veröffentlichen, um Änderungen auf den Katalog anzuwenden. Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Nachdem eine Maschine aktualisiert wurde, wird sie automatisch neu gestartet.

**Tipp:** Informationen zum Verwalten von Verbindungen finden Sie unter Verbindungen und Ressourcen.

Bevor Sie einen Maschinenkatalog aktualisieren, aktualisieren Sie zunächst ein vorhandenes Masterimage oder erstellen Sie ein neues auf dem Hypervisor.

1. Erstellen Sie auf dem Hypervisor bzw. im Clouddienst einen Snapshot der aktuellen VM und geben Sie diesem einen aussagekräftigen Namen. Der Snapshot kann notfalls zur Wiederherstellung (Rollback) der Maschinen in dem Katalog verwendet werden.
2. Falls erforderlich, schalten Sie das Masterimage ein und melden Sie sich an.
3. Installieren Sie Updates bzw. nehmen Sie die erforderlichen Änderungen am Masterimage vor.
4. Wenn das Masterimage eine persönliche vDisk verwendet, aktualisieren Sie den Bestand.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Wenden Sie die in den folgenden Leitfäden aufgeführten Optimierungen auf Ihre Umgebung an: Windows 7 Optimization Guide und Windows 8/8.1 Virtual Desktop Optimization Guide.
6. Schalten Sie die virtuelle Maschine aus.
7. Erstellen Sie einen Snapshot der VM und geben Sie diesem einen aussagekräftigen Namen, der bei der Aktualisierung des Katalogs in Studio erkannt wird. Obwohl Studio einen Snapshot erstellen kann, empfiehlt Citrix, dass Sie einen Snapshot mit der Hypervisor-Verwaltungskonsole erstellen und dann den Snapshot in Studio auswählen. Dadurch können Sie statt eines automatisch erstellten Namens einen aussagekräftigen Namen und eine Beschreibung zuweisen. Bei GPU-Masterimages können Sie das Masterimage nur über die XenServer XenCenter-Konsole ändern.

Vorbereiten und Verteilen des Updates auf allen Maschinen in einem Katalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie eine Maschine und dann im Aktionsbereich **Maschinen aktualisieren**.
3. Wählen Sie auf der Seite **Masterimage** den Host und das gewünschte Masterimage.
4. Legen Sie auf der Seite **Rolloutstrategie** fest, wann die Aktualisierung der Maschinen im Maschinenkatalog erfolgen soll: beim nächsten Herunterfahren oder sofort. Details hierzu finden Sie weiter unten.
5. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie dann auf **Fertig stellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet.

**Tipp:** Wenn Sie einen Katalog direkt mit dem PowerShell-SDK anstelle von Studio aktualisieren, können Sie alternativ zu einem Image bzw. einem Image-Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

## Rolloutstrategie

Ein Update des Images beim nächsten Herunterfahren wird angeboten, wenn Sie den Citrix Connector für System Center Configuration Manager verwenden.

Wenn Sie das Image sofort aktualisieren, konfigurieren Sie eine Zeit und Benachrichtigungen für die Verteilung.

- **Verteilungszeit:** Sie können alle Maschinen zur gleichen Zeit aktualisieren lassen oder eine Zeitdauer festlegen, während derer die Aktualisierung aller Maschinen im Katalog stattfinden soll. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums aktualisiert und neu gestartet wird.
- **Benachrichtigung:** Wählen Sie in dieser Dropdownliste aus, ob auf den Maschinen eine Meldung angezeigt werden soll, bevor das Update beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Update eine Meldung angezeigt wird, können Sie in der rechten Dropdownliste vorgeben, dass die Meldung alle fünf Minuten nach der Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt. Sofern Sie kein gleichzeitiges Update aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der von dem internen Algorithmus berechneten Zeit vor dem Update angezeigt.

Nach Bereitstellung eines aktualisierten/neuen Masterimages können Sie diese mit einem Rollback rückgängig machen. Dies kann erforderlich sein, wenn Probleme bei den aktualisierten Maschinen auftreten. Bei einem Rollback werden die Maschinen in dem Katalog auf das letzte funktionierende Image zurückgesetzt. Neue Features, die das neue Image erfordern, stehen dann nicht mehr zur Verfügung. Bei einem Rollback einer Maschine ist ein Neustart erforderlich.

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** aus.
2. Wählen Sie den Maschinenkatalog und dann im Aktionsbereich **Rollback für Maschinenupdate**.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

3. Legen Sie fest, wann das ältere Masterimage auf die Maschinen angewendet werden soll (gemäß den Rollout-Anweisungen oben).

Das Rollback wird nur auf Maschinen angewendet, die zurückgesetzt werden müssen. Benutzer von Maschinen, die nicht mit dem neuen/aktualisierten Masterimage aktualisiert wurden (z. B. weil sie sich nicht abgemeldet hatten), erhalten keine Meldung und müssen sich nicht abmelden.

# Durchführen eines Upgrades eines Maschinenkatalogs und Rückgängigmachen eines Upgrades

Aktualisieren Sie den Maschinenkatalog nach dem Upgrade der VDAs auf den Maschinen auf eine neuere Version. Citrix empfiehlt das Upgrade aller VDAs auf die aktuelle Version, damit Zugriff auf alle neuen Features besteht.

Upgradevorbereitung:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version in der Provisioning Services Console.
- Starten Sie die aktualisierten Maschinen, damit sie sich bei dem Controller registrieren. Auf diese Weise kann Studio feststellen, dass die Maschinen im Maschinenkatalog aktualisiert werden müssen.

Upgrade eines Maschinenkatalogs durchführen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie den Katalog aus. Auf der Registerkarte "Details" im unteren Bereich werden Versionsinformationen angezeigt.
3. Wählen Sie **Katalog aktualisieren**. Wenn Studio erkennt, dass für den Maschinenkatalog ein Upgrade erforderlich ist, wird eine Meldung angezeigt. Folgen Sie den Anweisungen. Kann eine Maschine nicht aktualisiert werden, wird eine Meldung mit einer Erläuterung der Ursache des Problems angezeigt. Citrix empfiehlt, dass Sie alle Maschinenprobleme beheben, bevor Sie den Maschinenkatalog aktualisieren, damit alle Maschinen einwandfrei funktionieren.

Wenn das Katalogupgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie den Maschinenkatalog und dann im Aktionsbereich **Rückgängig machen** wählen.

**Hinweis:** Für Windows XP- und Windows Vista-Maschinen muss eine ältere VDA-Version verwendet werden. Die Verwendung der neuesten Produktfeatures ist hier nicht möglich. Wenn Sie diese Maschinen nicht auf ein derzeit unterstütztes Windows-Betriebssystem aktualisieren können, empfiehlt Citrix, sie in einem separaten Maschinenkatalog zu führen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen von Bereitstellungsgruppen

Aug 17, 2016

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen bzw. Desktops für diese Benutzer verfügbar sein sollen.

Das Erstellen einer Bereitstellungsgruppe ist nach dem Erstellen einer Site und eines Maschinenkatalogs der nächste Schritt beim Konfigurieren der Bereitstellung. Später können Sie die anfänglichen Einstellungen der ersten Bereitstellungsgruppe ändern und weitere Bereitstellungsgruppen erstellen. Es gibt Features und Einstellungen, die Sie nur beim Bearbeiten einer Bereitstellungsgruppe, nicht aber beim Erstellen konfigurieren können.

Beim Erstellen einer Remote-PC-Zugriff-Site wird automatisch eine Bereitstellungsgruppe namens **Remote-PC-Zugriff-Desktops** erstellt.

Erstellen einer Bereitstellungsgruppe

1. Wenn Sie eine Site und einen Maschinenkatalog, jedoch noch keine Bereitstellungsgruppe erstellt haben, führt Studio Sie zum richtigen Startpunkt für die Erstellung einer Bereitstellungsgruppe. Wenn Sie bereits eine Bereitstellungsgruppe erstellt haben und eine weitere erstellen möchten, wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann im Aktionsbereich **Bereitstellungsgruppe erstellen**.
2. Der Assistent zum Erstellen von Bereitstellungsgruppen wird mit der Seite **Einführung** gestartet. Diese können Sie für künftige Starts des Assistenten unterdrücken.
3. Der Assistent führt Sie durch die nachfolgend beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur letzten Seite gelangen.

Wählen Sie einen Maschinenkatalog und die Anzahl der Maschinen, die Sie aus dem Katalog verwenden möchten.

Gut zu wissen:

- Mindestens eine Maschine in dem ausgewählten Katalog muss unbenutzt bleiben.
- Ein Maschinenkatalog kann in mehreren Bereitstellungsgruppen angegeben werden, eine Maschine kann jedoch nur in einer Bereitstellungsgruppe verwendet werden.
- Eine Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen verwenden, diese Kataloge müssen allerdings Maschinen desselben Typs enthalten (Serverbetriebssystemmaschinen oder Desktopbetriebssystemmaschinen oder Remote-PC-Zugriff-Maschinen). Sie können also in einer Bereitstellungsgruppe nicht verschiedene Maschinentypen mischen. Umfasst Ihre Bereitstellung Maschinenkataloge für Windows-Maschinen und solche für Linux-Maschinen, darf eine Bereitstellungsgruppe nur Maschinen eines Betriebssystems enthalten.
- Citrix empfiehlt, dass Sie alle Maschinen mit der neuesten VDA-Version installieren oder aktualisieren und dann das Upgrade von Maschinenkatalogen und Bereitstellungsgruppen nach Bedarf durchführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. (Dies wird als *Funktionsebene* der Gruppe bezeichnet.) Wenn auf einer der ausgewählten Maschinen beispielsweise ein VDA der Version 7.1 und auf den anderen die aktuelle VDA-Version installiert ist, können alle Maschinen der Gruppe nur die Features verwenden, die vom VDA der Version 7.1 unterstützt werden. Das bedeutet, dass einige Features, die neuere VDA-Versionen erfordern, in der Bereitstellungsgruppe möglicherweise nicht zur Verfügung stehen. Zur Verwendung von AppDisks müssen die VDAs (und


© 1999-2017 Citrix Systems, Inc. All rights reserved.

somit Funktionsebene der Gruppe) beispielsweise mindestens in Version 7.8 vorliegen.
- Alle Maschinen in einem Remote-PC-Zugriff-Maschinenkatalog werden automatisch einer Bereitstellungsgruppe zugewiesen. Wenn Sie eine Remote-PC-Zugriff-Site erstellen, werden automatisch ein Maschinenkatalog unter dem Namen **Remote-PC-Zugriff-Maschinen** und eine Bereitstellungsgruppe unter dem Namen **Remote-PC-Zugriff-Desktops** erstellt.

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit statischen (zugewiesen) Desktopbetriebssystemmaschinen auswählen. Wählen Sie auf der Seite "Bereitstellungstyp" entweder **Anwendungen** oder **Desktops**. Sie können nicht beide Optionen wählen.

Wenn Sie Maschinen aus einem Katalog mit Serverbetriebssystemmaschinen oder einem Katalog mit nach dem Zufallsprinzip zugewiesenen (gepoolten) Desktopbetriebssystemmaschinen ausgewählt haben, wird als Bereitstellungstyp "Anwendungen und Desktops" angenommen. Sie können Anwendungen, Desktops oder beides bereitstellen.

Klicken Sie auf **Hinzufügen**, um eine AppDisk hinzuzufügen. Im Dialogfeld "AppDisks auswählen" werden in der linken Spalte die verfügbaren AppDisks angezeigt. In der rechten Spalte werden die Anwendungen auf der jeweiligen AppDisk angezeigt. Auf der Registerkarte **Anwendungen** oberhalb der rechten Spalte werden die Anwendungen in Startmenüformat angezeigt, auf der Registerkarte **Installierte Pakete** ähnelt die Anzeige der Liste "Programme und Features".

Wählen Sie ein oder mehrere Kontrollkästchen.

Weitere Informationen finden Sie im Artikel AppDisks.

Geben Sie die Benutzer und Benutzergruppen an, die die Anwendungen und/oder Desktops in der Bereitstellungsgruppe verwenden können.

## Festlegung von Benutzerlisten

Active Directory-Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Benutzerzugriffsliste für eine Site, die nicht über Studio konfiguriert wird. Standardmäßig umfasst die Anwendungsanspruch-Richtlinienregel alle Benutzer (Einzelheiten s. BrokerAppEntitlementPolicyRule-Cmdlets des PowerShell-SDKs.
- Anwendungsgruppen (sofern konfiguriert)
- Bereitstellungsgruppen
- Anwendungen

Die Liste der Benutzer, die Zugriff auf eine Anwendung über StoreFront haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt. Beispiel: Konfigurieren der Verwendung von Anwendung A für eine bestimmte Abteilung, ohne den Zugriff auf andere Gruppen übermäßig einzuschränken:

- Verwenden Sie die Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt.
- Konfigurieren Sie die Benutzerliste der Bereitstellungsgruppe, sodass alle Firmensitz-Benutzer alle Anwendungen der Bereitstellungsgruppe verwenden können.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- (Wenn Anwendungsgruppen konfiguriert sind) Konfigurieren Sie die Benutzerliste der Anwendungsgruppe, sodass die Mitglieder der Verwaltung und Buchhaltung auf Anwendung A über L zugreifen können.
- Konfigurieren Sie die Eigenschaften von Anwendung A, sodass die Sichtbarkeit auf die Debitoren-Mitarbeiter in Verwaltung und Buchhaltung beschränkt ist.

## Authentifizierte und nicht authentifizierte Benutzer

Es gibt zwei Benutzertypen: authentifizierte und nicht authentifizierte Benutzer (nicht authentifizierte Benutzer werden auch als "anonyme" Benutzer bezeichnet). Konfigurieren einen oder beide Typen in einer Bereitstellungsgruppe konfigurieren.

### Authentifiziert

Die Benutzer und Gruppenmitglieder, die Sie namentlich festlegen, müssen für den Zugriff auf Anwendungen und Desktops in StoreFront oder Citrix Receiver Anmeldeinformationen, z. B. Smartcard oder Benutzernamen und Kennwort, angeben. (Bei Bereitstellungsgruppen mit Desktopbetriebssystemmaschinen können Sie eine Liste der Benutzer später unter Bearbeiten der Bereitstellungsgruppe importieren.)

### Nicht authentifiziert (anonym)

Bei Bereitstellungsgruppen mit Serverbetriebssystemmaschinen können Sie Benutzern Zugriff auf Anwendungen und Desktops gewähren, ohne dass die Benutzer Anmeldeinformationen in StoreFront oder Citrix Receiver eingeben müssen. Beispiel: Beim Zugriff über einen Kiosk werden für die Anwendung Anmeldeinformationen benötigt, nicht aber für das Citrix Zugriffsportal und Citrix Tools. Eine Gruppe anonymer Benutzer wird erstellt, wenn Sie den ersten Delivery Controller installieren.

Damit nicht authentifizierten Benutzern Zugriff erteilt werden kann, muss auf jeder Maschine in der Bereitstellungsgruppe ein VDA für Windows-Serverbetriebssysteme (mindestens Version 7.6) installiert sein. Wenn nicht authentifizierte Benutzer aktiviert sind, müssen Sie einen StoreFront-Store ohne Authentifizierung haben.

Nicht authentifizierte Benutzerkonten werden bei Bedarf beim Start einer Sitzung erstellt und "AnonXYZ" genannt (XYZ ist ein eindeutiger dreistelliger Wert).

Für Benutzersitzungen ohne Authentifizierung gilt ein Standardleerlauftimeout von 10 Minuten. Beim Trennen der Verbindung mit dem Client erfolgt automatisch die Abmeldung. Wiederverbindung, Roaming zwischen Clients und Workspace Control werden nicht unterstützt.

Die folgende Tabelle enthält die Optionen der Seite "Benutzer":

| Zugriff aktivieren für | Benutzer und Benutzergruppen hinzufügen/zuweisen? | Kontrollkästchen "Nicht authentifizierte Benutzer zulassen" aktivieren? |
|---|---|---|
| Nur authentifizierte Benutzer | Ja | Nein |
| Nur nicht authentifizierte Benutzer | Nein | Ja |
| Sowohl authentifizierte als auch nicht | Ja | Ja |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | | |
|---|---|---|
| authentifizierte Benutzer | | |

Gut zu wissen:

- Sie können Remote-PC-Zugriff-Bereitstellungsgruppen keine Anwendungen hinzufügen.
- Standardmäßig werden neu hinzugefügte Anwendungen in einem Ordner mit dem Namen "Applications" abgelegt. Sie können einen anderen Ordner angeben. Weitere Informationen finden Sie im Artikel "Verwalten von Anwendungen".
- Sie können die Eigenschaften von Anwendung beim Hinzufügen zu einer Bereitstellungsgruppe oder später ändern. Weitere Informationen finden Sie im Artikel "Verwalten von Anwendungen".
- Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie dies ablehnen, wird die Anwendung mit einem Suffix hinzugefügt, sodass ihr Name innerhalb des Ordners eindeutig ist.
- Wenn Sie eine Anwendung mehreren Bereitstellungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Bereitstellungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Bereitstellungsgruppen, denen die Anwendung hinzugefügt wurde.
- Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft Anwendungsname (Benutzer), sonst wird den Benutzern der Name in Receiver doppelt angezeigt.

Klicken Sie auf Sie die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Vom Startmenü:** Anwendungen, die auf vom Masterimage in dem ausgewählten Katalog erstellten Maschinen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit den erkannten Anwendungen geöffnet. Wählen Sie hier die gewünschten Anwendungen und klicken Sie auf **OK**.
- **Manuell:** Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **OK**.
- **Vorhandene:** Anwendungen, die der Site bereits hinzugefügt wurden, ggf. in einer anderen Bereitstellungsgruppe. Wenn Sie diese Quelle wählen, wird eine neue Seite mit den erkannten Anwendungen geöffnet. Wählen Sie hier die gewünschten Anwendungen und klicken Sie auf **OK**.
- **App-V**: Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Wählen Sie in der anschließend angezeigten Liste die gewünschten Anwendungen aus und klicken Sie auf **OK**. Weitere Informationen finden Sie im Artikel App-V.

Ist eine Anwendungsquelle oder Anwendung nicht verfügbar oder ungültig, wird sie nicht angezeigt oder kann nicht ausgewählt werden. Die Quelle **Vorhandene** ist beispielsweise nicht verfügbar, wenn der Site keine Anwendungen hinzugefügt wurden. Es kann auch sein, dass eine Anwendung nicht mit den auf Maschinen im ausgewählten Maschinenkatalog unterstützten Sitzungstypen kompatibel ist.

Der Titel dieser Seite hängt davon ab, welchen Maschinenkatalog Sie zuvor im Assistenten ausgewählt haben:

- Wenn Sie einen Maschinenkatalog mit gepoolten Maschinen gewählt haben, lautet der Titel "Desktops".
- Wenn Sie einen Maschinenkatalog mit zugewiesenen Maschinen gewählt und auf der Seite "Bereitstellungstyp" "Desktops" gewählt haben, lautet der Titel "Desktopbenutzerzuweisungen".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Wenn Sie einen Maschinenkatalog mit zugewiesenen Maschinen gewählt und auf der Seite "Bereitstellungstyp" "Anwendungen" gewählt haben, lautet der Titel "Anwendungsbenutzerzuweisungen".

Klicken Sie auf **Add**. Führen Sie folgende Aktionen im Dialogfeld aus:

- Geben Sie in den Feldern "Anzeigename" und "Beschreibung" die Informationen ein, die in Receiver angezeigt werden sollen.
- Geben Sie über die Optionsfelder an, wer einen Desktop starten kann (bei Gruppen mit gepoolten Maschinen) bzw. wem eine Maschine zugewiesen werden soll, wenn er den Desktop startet (bei Gruppen mit zugewiesenen Maschinen). Es können entweder alle Benutzer mit Zugriff auf die Bereitstellungsgruppe oder bestimmte Benutzer und Benutzergruppen ausgewählt werden.
- Wenn die Gruppe zugewiesene Maschinen enthält, geben Sie die maximale Anzahl Desktops pro Benutzer an. Sie müssen 1 oder einen höheren Wert eingeben.
- Aktivieren oder deaktivieren Sie den Desktop (bei gepoolten Maschinen) bzw. die Desktopzuordnungsregel (bei zugewiesenen Maschinen). Durch Deaktivieren eines Desktops wird dieser nicht mehr bereitgestellt, durch Deaktivieren einer Desktopzuordnungsregel wird die automatische Desktopzuweisung beendet.
- Wenn Sie mit dem Dialogfeld fertig sind, klicken Sie auf **OK**.

Geben Sie einen Namen für die Bereitstellungsgruppe ein. Sie können optional eine Beschreibung eingeben, die in Receiver und Studio angezeigt wird.

Lesen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**. Wenn Sie keine Anwendungen gewählt bzw. keinen Desktop zur Bereitstellung angeben haben, werden Sie gefragt, ob Sie fortfahren möchten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwalten von Bereitstellungsgruppen

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Ändern der Benutzereinstellungen für eine Bereitstellungsgruppe
- Hinzufügen und Entfernen von Benutzern zu bzw. aus Bereitstellungsgruppen
- Ändern des Bereitstellungstyps von Bereitstellungsgruppen
- Ändern der StoreFront-Adressen
- Durchführen eines Upgrades einer Bereitstellungsgruppe und Rückgängigmachen eines Bereitstellungsgruppenupgrades
- Verwalten von Remote-PC-Zugriff-Bereitstellungsgruppen
- Herunterfahren und Neustarten von Maschinen in einer Bereitstellungsgruppe
- Energieverwaltung für Maschinen in einer Bereitstellungsgruppe
- Erstellen eines Neustartzeitplans für Maschinen in einer Bereitstellungsgruppe
- Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus) in einer Bereitstellungsgruppe
- Ändern der Maschinen-Benutzer-Zuweisung in einer Bereitstellungsgruppe
- Ändern der maximalen Anzahl Maschinen pro Benutzer in einer Bereitstellungsgruppe
- Lastverwaltung von Maschinen in Bereitstellungsgruppen
- Entfernen von Maschinen aus Bereitstellungsgruppen
- Einschränken des Zugriffs auf Maschinen einer Bereitstellungsgruppe
- Aktualisieren einer Maschine in einer Bereitstellungsgruppe
- Abmelden oder Trennen einer Sitzung oder Senden einer Nachricht an Benutzer einer Bereitstellungsgruppe
- Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen


# Einführung

In diesem Artikel werden die Schritte zum Verwalten von Bereitstellungsgruppen beschrieben. Sie können die Einstellungen ändern, die Sie beim Erstellen der Gruppe gewählt haben, und Sie können weitere Einstellungen konfigurieren, die beim Erstellen von Bereitstellungsgruppen nicht zur Verfügung stehen.

Informationen zum Verwalten von Anwendungen in Bereitstellungsgruppen finden Sie in dem Artikel über Anwendungen, einschließlich Informationen zum Hinzufügen und Entfernen von Anwendungen in einer Bereitstellungsgruppe und zum Ändern der Anwendungseigenschaften.

Das Verwalten von Bereitstellungsgruppen erfordert die Berechtigungen für delegierte Administration der integrierten Bereitstellungsgruppen-Administratorrolle. Weitere Informationen finden Sie im Artikel Delegierte Administration.

# Ändern der Benutzereinstellungen für eine Bereitstellungsgruppe

Der Name dieser Seite kann **Benutzereinstellungen** oder **Grundeinstellungen** lauten.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Ändern Sie auf der Seite **Benutzereinstellungen** (bzw. **Grundeinstellungen**), die folgenden Optionen nach Bedarf.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

| Einstellung | Beschreibung |
|---|---|
| Beschreibung | Text in StoreFront, der Benutzern angezeigt wird |
| Bereitstellungsgruppe aktivieren | Zeigt an, ob die Bereitstellungsgruppe aktiviert ist. |
| Desktops pro Benutzer | (Nur zugewiesene Desktopbetriebssystemmaschinen) Maximale Anzahl freigegebener Desktops, die ein Benutzer gleichzeitig aktiv haben darf. Bei Bereitstellungen mit Zuweisung bei der ersten Verwendung gibt dieser Wert an, wie viele Desktops Benutzer sich selbst zuweisen können. |
| Zeitzone | |
| Secure ICA aktivieren | Schützt die Kommunikation zwischen Maschinen in der Bereitstellungsgruppe mit SecureICA, wodurch das ICA-Protokoll verschlüsselt wird (Standardverschlüsselungsgrad ist 128 Bit, dieser kann mit dem SDK geändert werden). Citrix empfiehlt die Verwendung zusätzlicher Verschlüsselungsmethoden, z. B. TLS-Verschlüsselung, wenn Datenübertragungen über öffentliche Netzwerke stattfinden. Bei SecureICA wird die Datenintegrität auch nicht geprüft. |

# Hinzufügen und Entfernen von Benutzern zu bzw. aus Bereitstellungsgruppen

Ausführliche Informationen zu Benutzern finden Sie im Abschnitt "Benutzer" des Artikels "Erstellen von Bereitstellungsgruppen".

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Zum Hinzufügen von Benutzern klicken Sie auf der Seite **Benutzer** auf **Hinzufügen** und geben Sie die Benutzer an, die Sie hinzufügen möchten. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und klicken Sie auf **Entfernen**. Sie können auch den Zugriff nicht authentifizierter Benutzer über das entsprechende Kontrollkästchen aktivieren oder deaktivieren.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bei Bereitstellungsgruppen mit physischen Desktopbetriebssystemmaschinen können Sie Benutzerinformationen nach dem Erstellen der Bereitstellungsgruppe aus einer CSV-Datei importieren. Sie können Benutzerinformationen auch in eine CSV-Datei exportieren. Die CSV-Datei kann Daten aus einer vorherigen Produktversion enthalten.

Die erste Zeile der CSV-Datei muss durch Trennzeichen getrennte Spaltenüberschriften (in beliebiger Reihenfolge) enthalten, z. B. ADComputerAccount, AssignedUser, VirtualMachine und HostId. Die nachfolgenden Zeilen enthalten durch Trennzeichen getrennte Daten. Die Einträge unter ADComputerAccount können allgemeine Namen, IP-Adressen Distinguished Names oder Domänen-/Computernamenpaare sein.

Importieren oder Exportieren von Benutzerinformationen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Klicken Sie auf der Seite **Maschinenzuteilung** auf **Liste importieren** bzw. **Liste exportieren** und navigieren Sie zum Speicherort der Datei.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

# Ändern des Bereitstellungstyps von Bereitstellungsgruppen

Der Bereitstellungstyp bestimmt, was eine Gruppe bereitstellen kann: Anwendungen, Desktops oder beides.

Bevor Sie eine Bereitstellungsgruppe des Typs **Nur Anwendungen** oder **Desktops und Anwendungen** in eine Bereitstellungsgruppe des Typs **Nur Desktops** ändern, löschen Sie alle Anwendungen aus der Bereitstellungsgruppe.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Bereitstellungstyp** den gewünschten Bereitstellungstyp.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

# Ändern der StoreFront-Adressen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **StoreFront** die StoreFront-URLs aus (bzw. fügen Sie sie hinzu), die von der auf jeder Maschine in der Bereitstellungsgruppe installierten Citrix Receiver-Instanz verwendet werden sollen.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Sie können die StoreFront-Serveradresse auch festlegen, indem Sie im Studio-Navigationsbereich **Konfiguration** > **StoreFront** auswählen.

# Durchführen eines Upgrades einer


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bereitstellungsgruppe und Rückgängigmachen eines Bereitstellungsgruppenupgrades

Nach dem Upgrade der VDAs auf Maschinen einer Bereitstellungsgruppe sowie den Maschinen in den von ihr verwendeten Maschinenkatalogen führen Sie ein Upgrade der Bereitstellungsgruppe durch.

Führen Sie vor dem Upgrade der Bereitstellungsgruppe folgende Schritte durch:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version in der Provisioning Services Console.
- Starten Sie die Maschinen mit dem aktualisierten VDA, damit sie sich bei dem Delivery Controller registrieren können. Dadurch wird Studio darüber informiert, welche Elemente in der Bereitstellungsgruppe aktualisiert werden müssen.
- Wenn Sie ältere VDA-Versionen weiterverwenden müssen, sind neuere Produktfeatures ggf. nicht verfügbar. Weitere Informationen finden Sie in den Artikeln zu Upgrades.

Bereitstellungsgruppen aktualisieren:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Upgrade von Bereitstellungsgruppe durchführen**. Die Aktion **Upgrade von Bereitstellungsgruppe durchführen** wird nur angezeigt, wenn Studio aktualisierte VDAs erkennt.

Vor dem Starten des Upgrades wird in Studio gemeldet, welche Maschinen nicht aktualisiert werden können (falls es solche gibt) und warum. Sie können das Upgrade dann abbrechen, die Ursachen beheben und das Upgrade erneut starten.

Wenn das Upgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie die Bereitstellungsgruppe und dann im Aktionsbereich **Rückgängig machen** wählen.

# Verwalten von Remote-PC-Zugriff-Bereitstellungsgruppen

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs keinem Benutzer zugewiesen wurde, weist Studio sie vorübergehend einer Bereitstellungsgruppe zu, die dem Maschinenkatalog zugeordnet ist. Dadurch kann sie später einem Benutzer zugewiesen werden.

Die Zuweisung der Bereitstellungsgruppe zum Maschinenkatalog ist mit einem Prioritätswert verbunden. Die Priorität bestimmt, welcher Bereitstellungsgruppe eine Maschine zugewiesen ist, die bei der Registrierung beim System oder wenn ein Benutzer eine Maschinenzuweisung benötigt: je geringer der Wert, desto höher die Priorität. Wenn ein Remote-PC-Zugriff-Maschinenkatalog mehrere Bereitstellungsgruppenzuweisungen hat, wird die mit der höchsten Priorität vom System ausgewählt. Sie können die Priorität mit dem PowerShell-SDK festlegen.

Beim Erstellen eines Remote-PC-Zugriff-Maschinenkatalogs wird dieser einer Bereitstellungsgruppe zugeordnet. Dies bedeutet, dass dem Maschinenkatalog später hinzugefügte Maschinenkonten oder Organisationseinheiten in der Bereitstellungsgruppe hinzugefügt werden können. Die Zuordnung kann deaktiviert oder aktiviert werden.

Zuordnung eines Remote-PC-Zugriff-Maschinenkatalogs zu einer Bereitstellungsgruppe hinzufügen oder entfernen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Remote-PC-Zugriff-Gruppe aus.
3. Wählen Sie im Abschnitt "Details" die Registerkarte **Maschinenkataloge** und dann einen Remote-PC-Zugriff-Maschinenkatalog.
4. Um eine Zuordnung hinzuzufügen oder wiederherzustellen, wählen Sie **Desktops hinzufügen**. Zum Entfernen einer Zuordnung wählen Sie **Zuordnung entfernen**.

# Herunterfahren und Neustarten von Maschinen in einer Bereitstellungsgruppe

Dieser Vorgang wird für Remote-PC-Zugriff-Maschinen nicht unterstützt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie die Maschine und anschließend im Aktionsbereich eine der folgenden Optionen (einige Optionen sind je nach Maschinenzustand ggf. nicht verfügbar):

- **Herunterfahren erzwingen**: Das Abschalten der Maschine wird erzwungen und die Liste der Maschinen wird aktualisiert.
- **Neu starten:** Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt die Maschine im aktuellen Zustand.
- **Neustart erzwingen** Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet.
- **Anhalten:** Die Maschine wird angehalten, ohne sie herunterzufahren, und die Liste der Maschinen aktualisiert.
- **Herunterfahren:** Das Betriebssystem wird heruntergefahren.

Wird bei Aktionen ohne Erzwingen eine Maschine nicht innerhalb von 10 Minuten heruntergefahren, wird sie ausgeschaltet. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Citrixempfiehlt, dass Sie das Herunterfahren von Desktopbetriebssystemmaschinen durch Benutzer während einer Sitzung nicht zulassen. Einzelheiten finden Sie in der Microsoft-Dokumentation zu Richtlinien.

Sie können auch Maschinen einer Verbindung herunterfahren und neu starten. Informationen dazu finden Sie im Artikel über Verbindungen und Ressourcen.

# Energieverwaltung für Maschinen in einer Bereitstellungsgruppe

Die Energieverwaltung ist nur bei virtuellen Desktopbetriebssystemmaschinen, nicht aber bei physischen Maschinen (einschließlich Remote-PC-Zugriff-Maschinen) möglich. Desktopbetriebssystemmaschinen mit GPU-Funktionen können nicht angehalten werden, sodass Energieverwaltungsvorgänge fehlschlagen. Für Serverbetriebssystemmaschinen können Sie einen Neustartzeitplan erstellen. Das Verfahren wird im vorliegenden Abschnitt beschrieben.

In Bereitstellungsgruppen mit gepoolten Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Zustände annehmen:

- Zufällig zugewiesen und in Verwendung
- Nicht zugewiesen und nicht verbunden

In Bereitstellungsgruppen mit statischen Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden Zustände aufweisen:

- Dauerhaft zugeordnet und in Verwendung
- Dauerhaft zugewiesen und nicht verbunden (aber bereit für Verbindungen)
- Nicht zugewiesen und nicht verbunden

Statische Bereitstellungsgruppen enthalten im Normalbetrieb sowohl dauerhaft zugewiesene als auch nicht zugewiesene Maschinen. Anfangs sind alle Maschinen nicht zugewiesen (außer beim Erstellen der Bereitstellungsgruppe manuell zugewiesene Maschinen). Wenn Benutzer eine Verbindung herstellen, werden Maschinen dauerhaft zugewiesen. Die Energieverwaltung ist bei nicht zugewiesenen Maschinen in den Bereitstellungsgruppen vollständig, bei dauerhaft zugewiesenen Maschinen nur teilweise möglich.

**Pools und Puffer**: Unter einem Pool versteht man bei gepoolten Bereitstellungsgruppen und statischen Bereitstellungsgruppen mit nicht zugewiesenen Maschinen eine Gruppe nicht zugewiesener (oder temporär zugewiesener) Maschinen, die eingeschaltet bleiben und mit denen Benutzer eine Verbindung herstellen können (eine Maschine ist direkt nach der Anmeldung verfügbar). Die Poolgröße (d. h. die Zahl der Maschinen, die eingeschaltet bleiben) kann abhängig von der Tageszeit konfiguriert werden. Verwenden Sie zum Konfigurieren des Pools bei statischen Bereitstellungsgruppen das SDK.

Ein Puffer ist eine zusätzliche Gruppe nicht zugewiesener Maschinen, die eingeschaltet werden, wenn die Anzahl der Maschinen im Pool unter einen Schwellenwert (Prozentsatz der Größe der Bereitstellungsgruppe) fällt. Für große Bereitstellungsgruppen wird unter Umständen eine große Zahl Maschinen eingeschaltet, wenn der Schwellenwert unterschritten wird. Planen Sie die Größe Ihrer Bereitstellungsgruppen daher sorgfältig oder passen Sie die Standardpuffergröße mit dem SDK an.

**Energiestatustimer**: Sie können mit den Energiestatustimern Maschinen anhalten, wenn die Verbindung eine bestimmte Zeit lang getrennt war. Maschinen werden zum Beispiel automatisch außerhalb der Bürostunden angehalten, wenn die Verbindung mindestens 10 Minuten lang getrennt war. Zufällige Maschinen oder Maschinen mit persönlichen vDisks werden bei Abmeldung des Benutzers automatisch heruntergefahren, es sei denn, Sie konfigurieren die Bereitstellungsgruppeneigenschaft "ShutdownDesktopsAfterUse" im SDK.

Sie können Timer für Werktage und Wochenenden sowie für Spitzen- und Nebenzeiten konfigurieren.

**Teilweise Energieverwaltung bei dauerhaft zugewiesenen Maschinen**: Bei dauerhaft zugewiesenen Maschinen können Sie Energiestatustimer, aber keine Pools oder Puffer einrichten. Die Maschinen werden zu Beginn jeder Spitzenzeit eingeschaltet und zu Beginn eines Zeitraums mit geringer Auslastung ausgeschaltet. Es ist keine Feinsteuerung der Zahl der Maschinen möglich, die als Ausgleich für verwendete Maschinen verfügbar werden (im Gegensatz zu nicht zugewiesenen Maschinen).

Einstellen der Energieverwaltung für Desktopbetriebssystemmaschinen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Energieverwaltung** im Dropdownmenü "Energieverwaltung für Maschinen" die Option

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

**Werktage** aus. Wochentage umfassen standardmäßig die Tage von Montag bis Freitag.

4. Wählen Sie bei zufälligen Bereitstellungsgruppen unter **Maschinen einschalten** die Option **Bearbeiten** und geben Sie die Poolgröße während der Werktage an. Wählen Sie anschließend die Anzahl der einzuschaltenden Maschinen.
5. Legen Sie unter **Spitzenzeiten** die Zeiträume für Spitzen- und Nebenzeiten für jeden Tag fest.
6. Stellen Sie die Energiestatustimer für Spitzen- und Nebenzeiten an Werktagen ein: Geben Sie für **Während Spitzenzeiten > Wenn getrennt** die Verzögerung in Minuten ein, nach der getrennte Maschinen in der Bereitstellungsgruppe angehalten werden sollen, und klicken Sie auf "Anhalten". Geben Sie für **Während Nicht-Spitzenzeiten > Wenn getrennt** die Verzögerung in Minuten ein, nach der abgemeldete Maschinen in der Bereitstellungsgruppe heruntergefahren werden, und klicken Sie auf **Herunterfahren**. Dieser Timer ist für Bereitstellungsgruppen mit zufälligen Maschinen nicht verfügbar.
7. Wählen Sie im Dropdownmenü "Energieverwaltung für Maschinen" die Option **Wochenende** aus und konfigurieren Sie die Spitzenzeiten und Energiestatustimer für Wochenenden.
8. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Verwenden Sie das SDK für Folgendes:

- Herunterfahren anstelle von Anhalten von Maschinen basierend auf Energiestatustimern, oder wenn Timer auf Abmeldungen anstatt von Verbindungstrennungen reagieren sollen
- Ändern der Standardeinstellungen für Werktage und Wochenende

# Erstellen eines Neustartzeitplans für Maschinen in einer Bereitstellungsgruppe

Über einen Neustartzeitplan wird der regelmäßige Neustart aller Maschinen in einer Bereitstellungsgruppe festgelegt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wenn Sie nicht möchten, dass die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie auf der Seite **Neustartzeitplan** das Optionsfeld **Nein** und fahren Sie mit dem letzten Schritt dieses Verfahrens fort. Es wird kein Neustartzeitplan bzw. keine Rolloutstrategie konfiguriert. Wenn Sie zuvor einen Zeitplan konfiguriert hatten, wird er durch diese Auswahl aufgehoben.
4. Sollen die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie das Optionsfeld **Ja**.
5. Wählen Sie für **Neustartintervall** die Option **Täglich** oder den Wochentag, an dem der Neustart durchgeführt werden soll.
6. Wählen Sie für **Neustart beginnen um** die Tageszeit im 24-Stunden-Format, zu der der Neustart beginnen soll.
7. Wählen Sie unter **Neustartdauer** aus, ob alle Maschinen gleichzeitig gestartet werden sollen oder geben Sie die Gesamtzeitdauer zum Beginnen des Neustarts an. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums neu gestartet wird.
8. Wählen Sie in der Dropdownliste **Benachrichtigung** aus, ob auf den betroffenen Maschinen eine Meldung angezeigt werden soll, bevor der Neustart beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Neustart eine Meldung angezeigt wird, können Sie in der Dropdownliste **Benachrichtigung erneut senden** vorgeben, dass die Meldung alle fünf Minuten nach Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt.
9. Geben Sie im Feld **Benachrichtigung** den Text der Meldung ein (es gibt keinen Standardtext). Wenn die Meldung die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zeit in Minuten bis zum Neustart enthalten soll, verwenden Sie die Variable **%m%** (z. B. "Achtung: Der Computer wird in %m% Minuten automatisch neu gestartet.") Wenn Sie die Benachrichtigung wiederholen lassen und die Variable "%m%" verwenden, wird die Zeitangabe bei jeder Wiederholung um fünf Minuten verringert. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine in der Bereitstellungsgruppe zu der von dem internen Algorithmus berechneten Zeit angezeigt.

10. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Sie können kein automatisiertes Einschalten oder Herunterfahren über Studio durchführen, sondern nur Neustarts.

# Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus) in einer Bereitstellungsgruppe

Wenn Sie vorübergehend verhindern möchten, dass neue Verbindungen mit Maschinen hergestellt werden, können Sie den Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe aktivieren. Das ist beispielsweise vor dem Anwenden von Patches oder der Verwendung von Verwaltungstools nützlich.

- Wenn sich eine Serverbetriebssystemmaschine im Wartungsmodus befindet, können Benutzer eine Verbindung mit vorhandenen Sitzungen herstellen, aber keine neuen Sitzungen starten.
- Bei einer Desktopbetriebssystemmaschine (oder einem Computer mit Remote-PC-Zugriff) im Wartungsmodus können Benutzer keine Verbindung herstellen. Aktuelle Verbindungen bleiben bis zur Trennung oder Abmeldung erhalten.

Wartungsmodus ein- oder ausschalten:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe wählen Sie im Aktionsbereich **Wartungsmodus einschalten**. Zum Aktivieren des Wartungsmodus für einzelne Maschinen wählen Sie im Aktionsbereich **Maschinen anzeigen**. Wählen Sie eine Maschine aus und wählen Sie dann im Aktionsbereich **Wartungsmodus einschalten**.
4. Zum Deaktivieren des Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe befolgen Sie die Anweisungen oben unter Auswahl der Option **Wartungsmodus ausschalten** im Aktionsbereich.

Einstellungen für Windows-Remotedesktopverbindungen wirken sich auch darauf aus, ob eine Serverbetriebssystemmaschine im Wartungsmodus ist. Der Wartungsmodus ist in folgenden Fällen aktiviert:

- Der Wartungsmodus wurde wie oben beschrieben aktiviert.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt und für den Anmeldemodus der Remotehostkonfiguration wurde **Neue Verbindungen zulassen, doch neue Anmeldungen verhindern** oder **Neue Verbindungen zulassen, doch Neuanmeldungen bis zum Neustart des Servers verweigern** gewählt.

Sie können auch den Wartungsmodus für eine Verbindung ein- und ausschalten, was sich auf die Maschine auswirkt, die die Verbindung verwendet, oder für einen Maschinenkatalog, was sich auf alle Maschinen in diesem auswirkt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Ändern der Maschinen-Benutzer-Zuweisung in einer Bereitstellungsgruppe

Sie können die Zuweisungen von Desktopbetriebssystemmaschinen, nicht aber die von Serverbetriebssystemmaschinen oder Maschinen, die mit Provisioning Services erstellt wurden, ändern.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus.
3. Wählen Sie im Aktionsbereich **Bereitstellungsgruppe bearbeiten** aus. Geben Sie die neuen Benutzer auf der Seite **Desktops** oder **Desktopzuweisungsregeln** an (nur eine dieser Seiten ist verfügbar und hängt vom Typ des Maschinenkatalogs ab, den die Bereitstellungsgruppe verwendet).
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

# Ändern der maximalen Anzahl Maschinen pro Benutzer

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Legen Sie auf der Seite **Desktopzuweisungsregeln** einen Wert für "Maximale Desktops pro Benutzer" fest.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

# Lastverwaltung von Maschinen in Bereitstellungsgruppen

Die Lastverwaltung ist nur bei Serverbetriebssystemmaschinen möglich.

Bei der Lastverwaltung wird die Serverlast gemessen und festgelegt, welcher Server unter den aktuellen Umgebungsbedingungen auszuwählen ist. Diese Auswahl basiert auf folgenden Faktoren:

**Wartungsmodusstatus des Servers**: Eine Serverbetriebssystemmaschine wird nur für den Lastausgleich berücksichtigt, wenn der Wartungsmodus für sie deaktiviert ist.

**Serverlastindex**: bestimmt, mit welcher Wahrscheinlichkeit ein Server, der Serverbetriebssystemmaschinen bereitstellt, Verbindungen erhält. Der Index basiert auf einer Kombination von Lastauswertungskriterien: Anzahl der Sitzungen sowie Einstellungen für Leistungswerte (z. B. CPU-, Datenträger- und Speichernutzung). Die die Lastauswertungskriterien werden in den Richtlinieneinstellungen für die Lastverwaltung festgelegt.

Sie können den Lastindex in Director, über die Suche in Studio und im SDK überwachen.

In Studio ist die Serverlastindexspalte standardmäßig ausgeblendet. Zum Anzeigen der Spalte wählen Sie eine Maschine,


© 1999-2017 Citrix Systems, Inc. All rights reserved.

klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift und wählen Sie "Spalte auswählen". Klicken Sie in der Kategorie "Maschine" auf Serverlastindex.

Verwenden Sie im SDK das Cmdlet "Get-BrokerMachine". Weitere Informationen finden Sie unter CTX202150.

Ein Serverlastindex von 10.000 bedeutet, dass der Server voll ausgelastet ist. Wenn keine anderen Server verfügbar sind, erhalten die Benutzer beim Starten einer Sitzung u. U. eine Meldung, dass der Desktop oder die Anwendung zurzeit nicht verfügbar ist.

**Richtlinieneinstellung "Toleranzwert für gleichzeitige Anmeldungen"**: maximale Anzahl gleichzeitiger Serveranmeldeanforderungen. (Diese Einstellung entspricht der Lastdrosselung in XenApp-Versionen vor 7.5.)

Wenn alle Server den Toleranzwert für gleichzeitige Anmeldungen erreichen oder überschreiten, wird die nächste Anmeldeanforderung dem Server mit der niedrigsten Anzahl ausstehender Anmeldungen zugewiesen. Wenn mehrere Server diese Kriterien erfüllen, wird der Server mit dem niedrigsten Lastindex ausgewählt.

# Entfernen von Maschinen aus Bereitstellungsgruppen

Beim Entfernen einer Maschine wird diese aus der Bereitstellungsgruppe gelöscht, jedoch nicht aus dem Maschinenkatalog, den die Bereitstellungsgruppe verwendet. Die Maschine steht daher für Zuweisungen zu anderen Bereitstellungsgruppen zur Verfügung.

Maschinen müssen heruntergefahren werden, bevor sie entfernt werden können. Wenn Sie vorübergehend verhindern möchten, dass Benutzer eine Verbindung mit der Maschine herstellen, während Sie sie löschen, setzen Sie die Maschine in den Wartungsmodus, bevor Sie sie herunterfahren.

Wenn Sie eine Maschine einem anderen Benutzer zuweisen, denken Sie daran, dass Maschinen persönliche Daten enthalten können. Es empfiehlt sich ggf. ein Reimaging der Maschine.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im Aktionsbereich **Maschinen anzeigen**.
3. Stellen Sie sicher, dass die Maschine heruntergefahren ist.
4. Wählen Sie im Aktionsbereich **Aus Bereitstellungsgruppe entfernen**.

Sie können eine Maschine auch über die von der Maschine verwendete Verbindung aus einer Bereitstellungsgruppe entfernen. Weitere Informationen finden Sie im Artikel zu Verbindungen und Ressourcen.

# Einschränken des Zugriffs auf Maschinen einer Bereitstellungsgruppe

Alle Änderungen zum Einschränken des Zugriffs auf Maschinen in einer Bereitstellungsgruppe haben Vorrang vor zuvor durchgeführten Einstellungen, unabhängig von der verwendeten Methode. Sie haben folgende Möglichkeiten:

**Einschränken des Zugriffs für Administratoren über Geltungsbereiche für die delegierte Administration**. Sie können einen Geltungsbereich erstellen und zuweisen, in dem Administratoren auf alle Anwendungen zugreifen können, und einen zweiten Geltungsbereich, der nur den Zugriff auf spezifische Anwendungen zulässt. Weitere Informationen finden Sie im Artikel "Delegierte Administration".

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

**Einschränken des Zugriffs für Benutzer über SmartAccess-Richtlinienausdrücke**, mit denen über NetScaler Gateway hergestellte Benutzerverbindungen gefiltert werden.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Zugriffsrichtlinie** die Option **Über NetScaler Gateway hergestellte Verbindungen** aus.
4. Wenn Sie nur einen Teil dieser Verbindungen auswählen möchten, wählen Sie **Verbindungen, auf die mindestens einer der folgenden Filter zutrifft**. Legen Sie dann die NetScaler Gateway-Site fest und fügen Sie SmartAccess-Richtlinienausdrücke für zulässige Benutzerzugriffsszenarios hinzu, bzw. bearbeiten oder löschen Sie diese. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Gateway.
5. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

**Einschränken des Zugriffs für Benutzer über Ausschlussfilter** für mit dem SDK festgelegte Zugriffsrichtlinien. Zugriffsrichtlinien werden auf Bereitstellungsgruppen angewendet, um Verbindungen genauer zu definieren. Sie können beispielsweise den Maschinenzugriff für eine Untergruppe von Benutzern einschränken und zulässige Benutzergeräte festlegen. Mit Ausschlussfiltern können Zugriffsrichtlinien weiter angepasst werden. Aus Sicherheitsgründen können Sie beispielsweise den Zugriff für eine Untergruppe der Benutzer oder Geräte verweigern. Ausschlussfilter sind in der Standardeinstellung deaktiviert.

Wenn Sie beispielsweise den Zugriff von einem Lernlabor im Subnetz des Unternehmensnetzwerks auf eine spezifische Bereitstellungsgruppe verhindern möchten, unabhängig davon, wer die Maschinen im Labor nutzt, verwenden Sie folgenden Befehl: Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -

Sie können das Sternchen (*) als Platzhalter für alle Tags, die mit dem gleichen Richtlinienausdruck beginnen, verwenden. Wenn Sie beispielsweise auf einer Maschine das Tag "VPDesktops_Direct" hinzufügen und auf einer anderen das Tag "VPDesktops_Test", wird der Filter durch Festlegen des Tags auf "VPDesktops_*" im Skript "Set-BrokerAccessPolicy" auf beide Maschinen angewendet.

# Aktualisieren einer Maschine in einer Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und dann im Aktionsbereich **Maschinen aktualisieren**.

Zum Auswählen eines anderen Masterimages wählen Sie **Masterimage** und dann einen Snapshot.

Zum Anwenden der Änderungen und Benachrichtigen der Benutzer der Maschine wählen Sie **Rolloutbenachrichtigung für Endbenutzer**. Legen Sie anschließend Folgendes fest: ob die Aktualisierung des Masterimages sofort oder beim nächsten Neustart erfolgen soll, die Neustartverteilung (Gesamtzeit des Beginns der Aktualisierung aller Maschinen in der Gruppe) und ob Benutzer über den Neustart benachrichtigt werden sollen sowie die entsprechende Meldung.

# Abmelden oder Trennen einer Sitzung oder Senden


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# einer Nachricht an Benutzer einer Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Zum Abmelden einer Sitzung wählen Sie die Sitzung oder den Desktop und dann im Aktionsbereich **Abmelden**. Die Sitzung wird geschlossen und die Maschine steht nun anderen Benutzern zur Verfügung, sofern sie nicht einem bestimmten Benutzer zugewiesen ist.
4. Zum Trennen einer Sitzung wählen Sie die Sitzung oder den Desktop und dann im Aktionsbereich **Trennen**. Anwendungen werden weiter ausgeführt und die Maschine bleibt dem Benutzer zugewiesen. Der Benutzer kann eine Verbindung mit derselben Maschine wiederherstellen.
5. Zum Senden einer Nachricht an die Benutzer wählen Sie die Sitzung, die Maschine oder den Benutzer und dann im Aktionsbereich **Nachricht senden**. Geben Sie die Nachricht ein.

Sie können die Energiestatustimer für Desktopbetriebssystemmaschinen so konfigurieren, dass nicht genutzte Sitzungen automatisch verarbeitet werden. Einzelheiten finden Sie unter "Energieverwaltung für Maschinen".

# Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen in einer Bereitstellungsgruppe

Diese Features werden nur auf Serverbetriebssystemmaschinen unterstützt.

Vorabstart und Fortbestehen von Sitzungen ermöglichen einen schnellen Zugriff durch Benutzer auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden, und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat.

In der Standardeinstellung werden diese Features nicht verwendet, d. h. eine Sitzung startet, wenn ein Benutzer eine Anwendung startet, und bleibt so lange aktiv, bis die letzte Anwendung der Sitzung geschlossen wird.

Überlegungen:

- Die Bereitstellungsgruppe muss Anwendungen unterstützen und auf den Maschinen muss ein VDA für Windows-Serverbetriebssysteme in mindestens Version 7.6 ausgeführt werden.
- Diese Features werden nur bei Verwendung von Citrix Receiver für Windows unterstützt, sie erfordern außerdem zusätzliche Citrix Receiver-Konfigurationsschritte. Anweisungen hierzu finden Sie in der Produktdokumentation zu Ihrer Citrix Receiver für Windows-Version. Suchen Sie dort nach"Sitzungsvorabstart".
- Citrix Receiver für HTML5 wird nicht unterstützt.
- Wird ein Computer in den Modus "Anhalten" oder in den Ruhezustand versetzt, funktioniert der Sitzungsvorabstart unabhängig von den Vorabstarteinstellungen nicht. Die Benutzer können den Computer bzw. die Sitzung sperren, wenn sie sich jedoch von Citrix Receiver abmelden, wird die Sitzung beendet und ein Vorabstart ist nicht mehr möglich.
- Wird der Sitzungsvorabstart verwendet, können die Energieverwaltungsfunktionen "Anhalten" und "Ruhezustand" auf physischen Clientcomputern nicht verwendet werden. Clientmaschinenbenutzer können ihre Sitzungen sperren, sollten sich aber nicht abmelden.
- Vorab gestartete und fortbestehende Sitzungen verbrauchen eine Lizenz, jedoch nur wenn sie verbunden sind. Nicht


© 1999-2017 Citrix Systems, Inc. All rights reserved.

genutzte vorab gestartete und fortbestehende Sitzungen werden standardmäßig nach 15 Minuten getrennt. Dieser Wert kann über das PowerShell-Cmdlet "New/Set-BrokerSessionPreLaunch" konfiguriert werden.

- Eine sorgfältige Planung und Überwachung der Aktivitätsmuster von Benutzern ist wichtig, damit diese Features so eingerichtet werden können, dass sie einander ergänzen. In einer optimalen Konfiguration besteht ein Gleichgewicht zwischen dem Vorteil einer schnelleren Anwendungsverfügbarkeit für Benutzer und den durch den Verbrauch von Lizenzen und die fortdauernde Zuteilung von Ressourcen entstehenden Kosten.
- Sie können den Vorabstart von Sitzungen auch für eine spezifische Uhrzeit in Citrix Receiver konfigurieren.

Wie lange eine nicht genutzte Sitzung aktiv bleibt, wenn der Benutzer keine Anwendung startet, kann über ein Timeout oder über Serverlast-Schwellenwerte angegeben werden. Sie können alle Parameter konfigurieren und die Sitzung wird jeweils durch das zuerst auftretende Ereignis beendet.

- **Timeout:** Ein konfiguriertes Timeout gibt die Anzahl der Minuten, Stunden oder Tage an, die eine nicht genutzte vorab gestartete oder fortbestehende Sitzung aktiv bleibt. Wenn Sie ein zu kurzes Timeout konfigurieren, werden vorab gestartete Sitzungen beendet, bevor der Benutzer in den Genuss des schnelleren Anwendungszugriffs kommt. Ist das Timeout zu lang, werden eingehende Benutzerverbindungen möglicherweise abgewiesen, da der Server nicht genügend Ressourcen hat.

  Sie können dieses Timeout über das SDK (Cmdlet "New/Set-BrokerSessionPreLaunch"), nicht aber über Studio deaktivieren. Wenn Sie das Timeout deaktivieren, wird es für die betreffende Bereitstellungsgruppe in Studio und im Assistenten zum Bearbeiten von Bereitstellungsgruppen nicht angezeigt.

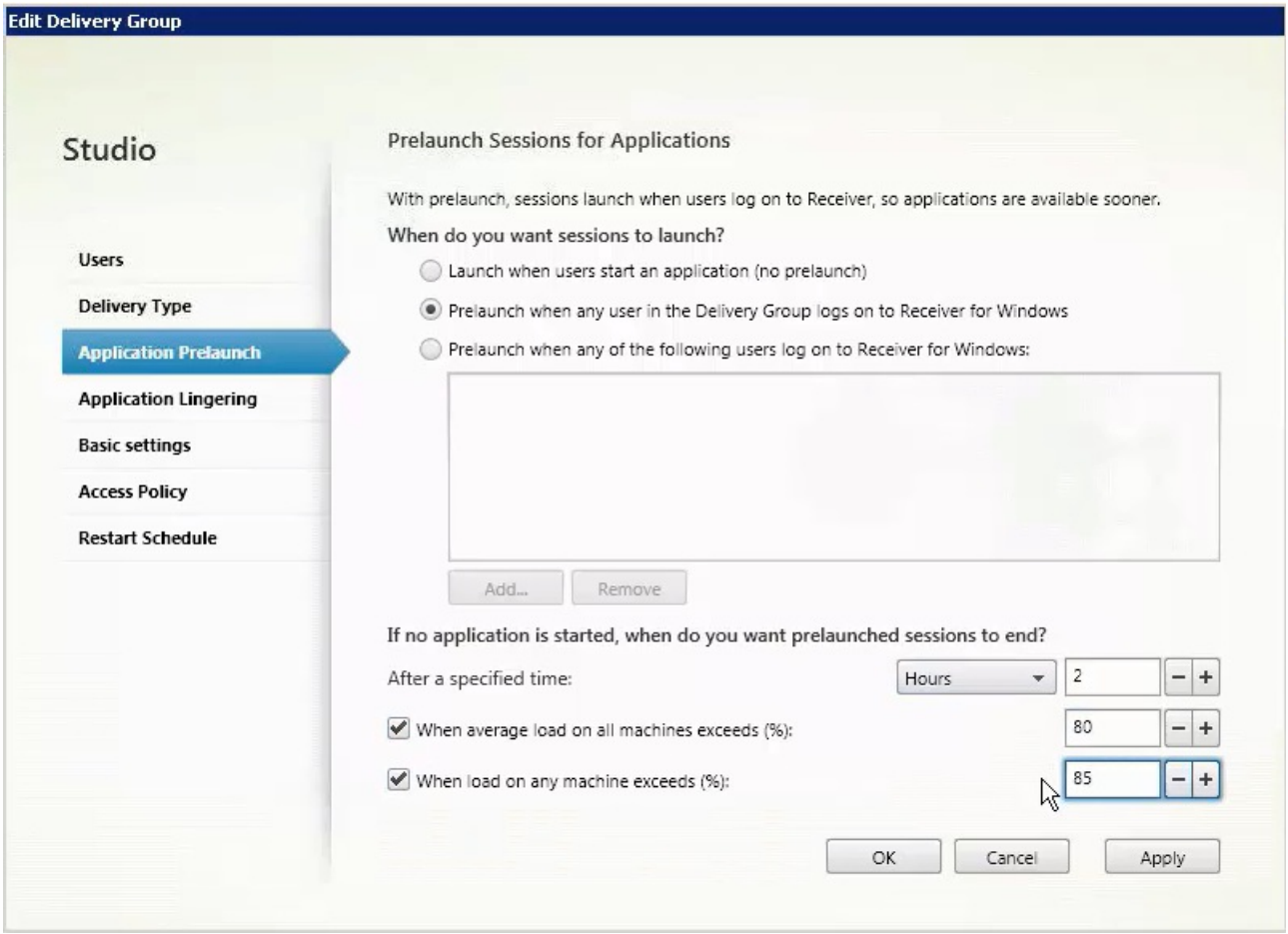
- **Schwellenwerte:** Das automatische Beenden vorab gestarteter und fortbestehender Sitzungen auf der Basis der Serverlast gewährleistet, dass Sitzungen so lange wie möglich geöffnet bleiben (vorausgesetzt, es sind Serverressourcen verfügbar). Nicht genutzte vorab gestartete und fortbestehende Sitzungen verursachen keine Abweisung von Verbindungen, da sie automatisch beendet werden, wenn Ressourcen für neue Benutzersitzungen benötigt werden.

  Sie können zwei Schwellenwerte konfigurieren: die durchschnittliche Last aller Server der Bereitstellungsgruppe und die höchste Last eines Servers in der Bereitstellungsgruppe (beides in Prozent). Wird ein Schwellenwert überschritten, werden jeweils die Sitzungen beendet, die sich am längsten im Zustand "vorab gestartet" bzw. "fortbestehend" befinden. Das Beenden erfolgt einzeln im Minutentakt bis die Last unter den Schwellenwert fällt. (Solange der Schwellenwert überschritten ist, werden keine neuen Sitzungen vorab gestartet.)

Server mit VDAs, die nicht beim Controller registriert sind, und Server im Wartungsmodus gelten als voll ausgelastet. Bei einem ungeplanten Ausfall werden vorab gestartete und fortbestehende Sitzungen automatisch beendet, um Kapazität freizugeben.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie den Vorabstart von Sitzungen, indem Sie auf der Seite **Anwendungsvorabstart** auswählen, wann Sitzungen gestartet werden sollen:
   - Wenn Benutzer eine Anwendung starten. Dies ist die Standardeinstellung. Der Vorabstart von Sitzungen ist deaktiviert.
   - Wenn ein Benutzer der Bereitstellungsgruppe sich bei Citrix Receiver für Windows anmeldet.
   - Wenn ein beliebiger Benutzer einer Liste mit Benutzern und Bereitstellungsgruppen sich bei Citrix Receiver für Windows anmeldet. Bei Auswahl dieser Option müssen Sie auch die Benutzer oder Benutzergruppen festlegen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

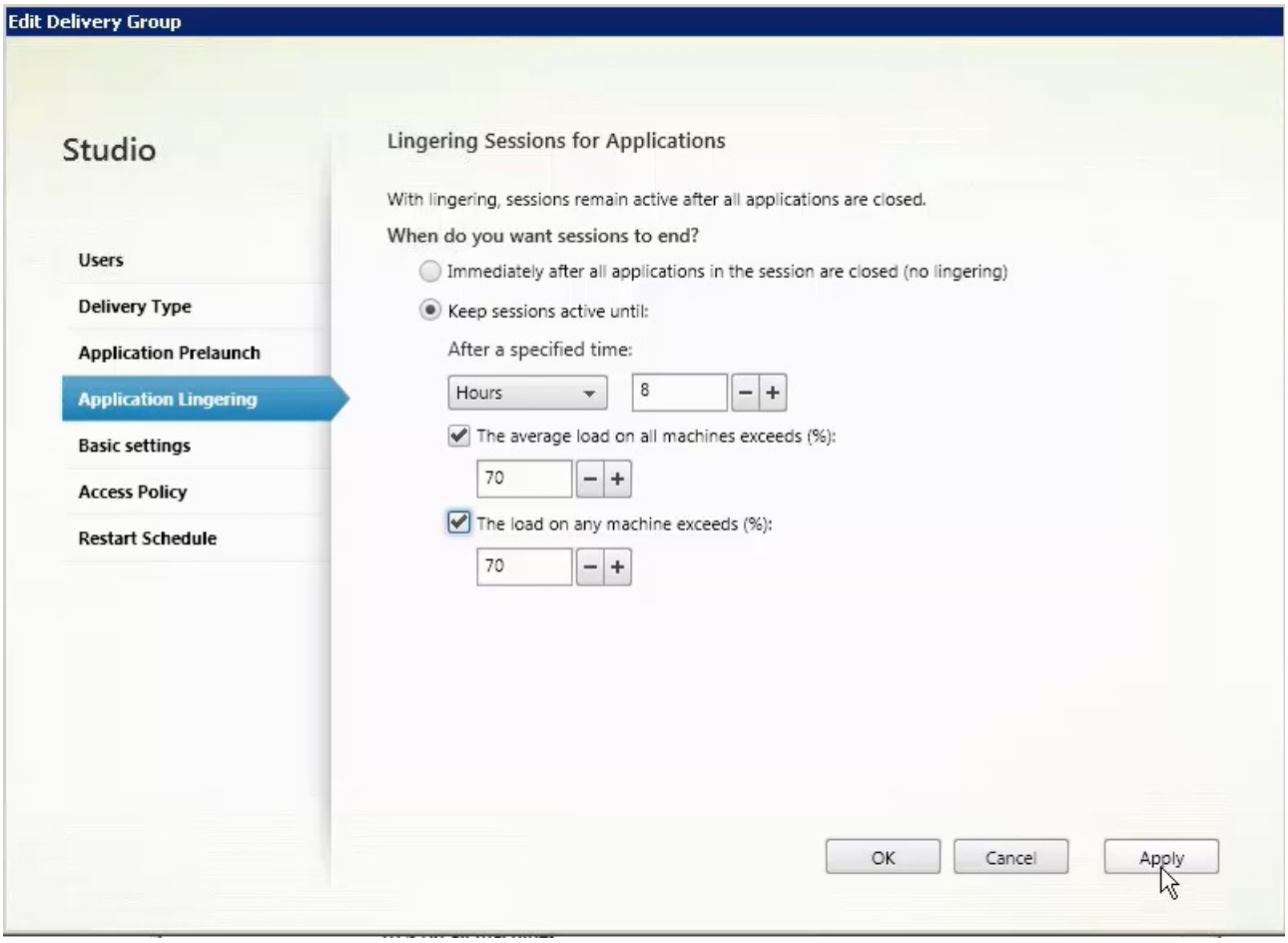



4. Eine vorab gestartete Sitzung wird durch eine normale Sitzung ersetzt, wenn der Benutzer eine Anwendung startet. Wenn der Benutzer keine Anwendung startet (d. h. die vorab gestartete Sitzung wird nicht verwendet), wird durch die folgenden Einstellungen bestimmt, wie lange die Sitzung aktiv bleibt.
   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

   Eine vorab gestartete Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Anwendungsfortbestehen** das Sitzungsfortbestehen durch Aktivieren des Optionsfelds **Sitzungen bleiben aktiv bis**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




4. Mehrere Einstellungen wirken sich darauf aus, wie lange eine Sitzung aktiv bleibt, wenn der Benutzer keine weitere Anwendung startet.
   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

   Eine fortbestehende Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen von Anwendungsgruppen

Jul 08, 2016

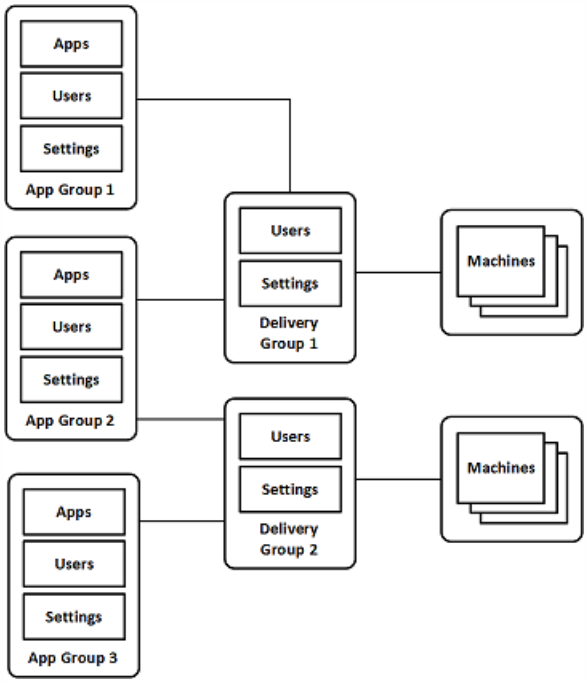
# Einführung

Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Anwendungsgruppen sind optional. Sie bieten eine Alternative zum Hinzufügen derselben Anwendungen zu mehreren Bereitstellungsgruppen. Bereitstellungsgruppen können mehreren Anwendungsgruppen und Anwendungsgruppen können mehreren Bereitstellungsgruppen zugeordnet werden.

Die Verwendung von Anwendungsgruppen kann für die Anwendungsverwaltung und Ressourcensteuerung gegenüber der Verwendung weiterer Bereitstellungsgruppen folgende Vorteile bieten:

- Durch die logische Gruppierung von Anwendungen und deren Einstellungen können Sie diese als Einheit verwalten. Sie müssen beispielsweise dieselbe Anwendung nicht mehreren Bereitstellungsgruppen einzeln hinzufügen (bzw. für diese veröffentlichen).
- Die Sitzungsfreigabe zwischen den Anwendungsgruppen kann Ressourcen sparen. In anderen Fällen ist das Deaktivieren der Sitzungsfreigabe zwischen Anwendungsgruppen möglicherweise nützlich.

Die folgende Abbildung zeigt eine XenApp- bzw. XenDesktop-Bereitstellung mit Anwendungsgruppen:




In dieser Konfiguration werden Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt. Über die Bereitstellungsgruppen wird festgelegt, welche Maschinen verwendet werden. (Obwohl dies nicht ausgezeichnet ist, sind die Maschinen in Maschinenkatalogen.)


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Anwendungsgruppe 1 ist Bereitstellungsgruppe 1 zugeordnet. Die Anwendungen in Anwendungsgruppe 1 sind für Benutzer der Anwendungsgruppe 1 zugänglich, sofern diese auch auf der Benutzerliste von Bereitstellungsgruppe 1 stehen. Diese Struktur folgt der Leitlinie, dass die Benutzerliste einer Anwendungsgruppe eine Teilgruppe (d. h. Einschränkung) der Benutzerlisten der zugeordneten Bereitstellungsgruppen sein muss. Die Einstellungen von Anwendungsgruppe 1 (Sitzungsfreigabe zwischen den Anwendungsgruppen, zugeordnete Bereitstellungsgruppen usw.) gelten für die Anwendungen und Benutzer in der Gruppe. Die Einstellungen in Bereitstellungsgruppe 1 (z. B. Unterstützung für anonyme Benutzer) gelten für die Benutzer in Anwendungsgruppe 1 und 2, da beide Anwendungsgruppen der Bereitstellungsgruppe zugeordnet sind.

Anwendungsgruppe 2 ist den Bereitstellungsgruppen 1 und 2 zugeordnet. Beiden Bereitstellungsgruppen kann in Anwendungsgruppe 2 eine Priorität zugewiesen werden, welche die Reihenfolge vorgibt, in der die Bereitstellungsgruppen beim Starten einer Anwendung geprüft werden. Für Bereitstellungsgruppen mit der gleichen Priorität findet ein Lastausgleich statt. Die Anwendungen in Anwendungsgruppe 2 sind für Benutzer der Anwendungsgruppe 2 zugänglich, sofern diese auch auf den Benutzerlisten von Bereitstellungsgruppe 1 und 2 stehen.

# Empfehlungen und Tipps

Citrix empfiehlt, Anwendungen entweder Anwendungsgruppen oder Bereitstellungsgruppen zuzuordnen, jedoch nicht beidem. Werden dieselben Anwendungen zwei Gruppentypen zugeordnet, kann dies die Verwaltung erschweren.

Standardmäßig sind Anwendungsgruppen aktiviert. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern (siehe Verwalten von Anwendungsgruppen).

Standardmäßig ist die Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert (siehe Sitzungsfreigabe zwischen Anwendungsgruppen weiter unten).

Citrix empfiehlt, Bereitstellungsgruppen auf die aktuelle Version zu aktualisieren. Dies erfordert (1) ein Upgrade der VDAs auf den Maschinen der Bereitstellungsgruppe, (2) ein Upgrade der Maschinenkataloge, in denen die Maschinen sind, und (3) das Upgrade der Bereitstellungsgruppe. Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen. Zur Verwendung von Anwendungsgruppen müssen die Kernkomponenten mindestens in Version 7.9 vorliegen.

Zum Erstellen von Anwendungsgruppen ist die Berechtigung zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Weitere Informationen finden Sie im Artikel Delegierte Administration.

In diesem Abschnitt wird der Begriff der Zuordnung von Anwendungen zu Anwendungsgruppen verwendet, um den Unterschied zum Hinzufügen einer neuen Anwendungsinstanz aus einer verfügbaren Quelle zu unterstreichen. Das Gleiche gilt für Bereitstellungsgruppen und Anwendungsgruppen. Diese werden einander zugeordnet und nicht als Komponenten hinzugefügt.

# Sitzungsfreigabe zwischen Anwendungsgruppen

Wenn Sie Anwendungsgruppen verwenden, können Sie die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen zulassen oder unterbinden. (Damit wird das bei ausschließlicher Verwendung von Bereitstellungsgruppen mögliche Standardverhalten der Sitzungsfreigabe wie im ersten Beispiel unten erläutert erweitert.) Die Anwendungssitzungsfreigabe spart die Kosten weiterer Anwendungssitzungsstarts. Außerdem ermöglicht sie die Verwendung von Anwendungsfeatures, bei denen die Zwischenablage genutzt wird, z. B. Kopieren und Einfügen.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Beispielszenario, in dem die Aktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:

> Ein Benutzer in Anwendungsgruppe 1 startet eine Anwendungssitzung mit Word. Während Word ausgeführt wird, startet er Excel. Findet der Controller Excel auf demselben Server, wird die Sitzung freigegeben. (Dies entspricht der einfachen Sitzungsfreigabe in Bereitstellungsgruppen, wenn keine Anwendungsgruppen verwendet werden.) Ist Excel nicht auf demselben Server und die Sitzungsfreigabe ist für Anwendungsgruppe 1 aktiviert, versucht der Controller, die Sitzung freizugeben, sofern die Anwendung auf einem anderen Server in den Anwendungsgruppe 1 zugeordneten Bereitstellungsgruppen oder in Anwendungsgruppe 2 oder 3 gefunden wird.

Beispielszenario, in dem die Deaktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:

> Sie haben einige Anwendungen, die mit anderen, auf denselben Maschinen installierten Anwendungen nicht gut zusammenarbeiten, z. B. zwei verschiedene Versionen der gleichen Software oder des gleichen Webbrowsers. Sie möchten nicht, dass ein Benutzer beide Versionen in derselben Sitzung startet.
>
> Sie erstellen mehrere Anwendungsgruppen und fügen jede Version der Software einer eigenen Anwendungsgruppe hinzu. Wenn die Sitzungsfreigabe zwischen diesen Anwendungsgruppen deaktiviert ist, können die in den Gruppen angegebenen Benutzer Anwendungen der gleichen Version in der gleichen Sitzung ausführen und sie können gleichzeitig andere Anwendungen ausführen, jedoch nicht in der gleichen Sitzung. Wenn ein Benutzer eine der in mehreren Versionen vorliegenden Anwendungen (die in verschiedenen Anwendungsgruppen sind) oder eine nicht in einer Anwendungsgruppe befindliche Anwendung startet, wird diese in einer neuen Sitzung gestartet.

**WICHTIG:** Die Sitzungsfreigabe zwischen Anwendungsgruppen ist keine Sicherheits-Sandbox. Sie ist nicht betriebssicher und kann nicht verhindern, dass Benutzer Anwendungen in ihren Sitzungen über andere Methoden (z. B. über Windows Explorer) starten.

Wenn eine Maschine unter Volllast steht, wird die Sitzungsfreigabe nicht zugelassen.

Sie müssen die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen aktivieren, wenn Sie Sitzungsvorabstart und Sitzungsfortbestehen verwenden möchten. Diese Features müssen jedoch in jeder den Anwendungsgruppen zugeordneten Bereitstellungsgruppe aktiviert und konfiguriert werden. Sie können sie nicht in den Anwendungsgruppen konfigurieren.

Die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Dies können Sie bei der Erstellung nicht ändern. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern (siehe Verwalten von Anwendungsgruppen).

# Erstellen von Anwendungsgruppen

Gehen Sie zum Erstellen von Anwendungsgruppen folgendermaßen vor:

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und im Aktionsbereich **Anwendungsgruppe erstellen**.
2. Der Assistent zum Erstellen von Anwendungsgruppen wird mit der Seite **Einführung** gestartet. Diese können Sie für künftige Starts des Assistenten unterdrücken.
3. Der Assistent führt Sie durch die nachfolgend beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur letzten Seite mit der Zusammenfassung gelangen.

Alle Bereitstellungsgruppen werden zusammen mit der Anzahl enthaltener Maschinen aufgelistet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Die Liste **Kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie auswählen können. Kompatible Bereitstellungsgruppen enthalten zufällige (nicht dauerhaft oder statisch zugewiesene) Server- oder Desktopbetriebssystemmaschinen.
- Die Liste **Nicht kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie nicht auswählen können. Jeder Eintrag enthält eine Begründung der Inkompatibilität, z. B. "enthält statisch zugewiesene Maschinen".

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn (1) die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren XenDesktop 7.x-Version erstellt wurde und (2) Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen" geändert, wenn für den Assistenten zum Erstellen von Anwendungsgruppen ein Commit ausgeführt wird.

Sie können Anwendungsgruppen erstellen, die keiner Bereitstellungsgruppe zugeordnet sind, z. B. zum Organisieren von Anwendungen oder als Speicher für Anwendungen, die gerade nicht verwendet werden. Anwendungsgruppen können jedoch erst dann zum Bereitstellen von Anwendungen verwendet werden, wenn sie mindestens einer Bereitstellungsgruppe zugeordnet sind. Sie können außerdem einer Anwendungsgruppe keine Anwendungen aus der Quelle "Vom Startmenü" hinzufügen, wenn keine Bereitstellungsgruppen festgelegt sind.

Über die Bereitstellungsgruppen legen Sie fest, welche Maschinen für die Bereitstellung von Anwendungen verwendet werden. Aktivieren Sie die Kontrollkästchen neben den Bereitstellungsgruppen, die Sie der Anwendungsgruppe zuordnen möchten.

Geben Sie an, wer die Anwendungen in der Anwendungsgruppe verwenden kann. Sie können entweder alle Benutzer und Gruppen in den Bereitstellungsgruppen, die Sie auf der vorherigen Seite ausgewählt haben, angeben oder bestimmte Benutzer bzw. Benutzergruppen aus den Bereitstellungsgruppen auswählen. Wenn Sie die Benutzer einschränken, haben nur die in der Bereitstellungsgruppe und der Anwendungsgruppe angegebenen Benutzer Zugriff auf die Anwendungen in der Anwendungsgruppe. Im Prinzip wirkt die Benutzerliste der Anwendungsgruppe als Filter für die Benutzerlisten in den Bereitstellungsgruppen.

Das Aktivieren oder Deaktivieren der Anwendungsverwendung durch nicht authentifizierte Benutzer ist nur über Bereitstellungsgruppen, nicht aber über Anwendungsgruppen möglich.

### Festlegung von Benutzerlisten

Active Directory-Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Benutzerzugriffsliste für eine Site, die nicht über Studio konfiguriert wird. Standardmäßig umfasst die Anwendungsanspruch-Richtlinienregel alle Benutzer (Einzelheiten s. BrokerAppEntitlementPolicyRule-Cmdlets des PowerShell-SDKs.
- Benutzerliste der Anwendungsgruppe
- Benutzerliste der Bereitstellungsgruppe
- Eigenschaft der Anwendungssichtbarkeit

Die Liste der Benutzer, die Zugriff auf eine Anwendung über StoreFront haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt. Wenn Sie beispielsweise die Verwendung von Anwendung A für eine bestimmte

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Abteilung konfigurieren möchten, ohne Zugriff für andere Gruppen unnötig einzuschränken, gehen Sie folgendermaßen vor:

- Verwenden der Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt
- Konfigurieren Sie die Benutzerliste der Bereitstellungsgruppe so, dass alle Benutzer der Organisation die Anwendungen der Bereitstellungsgruppe verwenden können.
- Konfigurieren Sie die Benutzerliste der Anwendungsgruppe so, dass die Mitarbeiter der Verwaltungs- und der Finanzabteilung Zugriff auf Anwendungen A bis L erhalten.
- Konfigurieren Sie die Eigenschaften von Anwendung A so, dass sie nur für Mitarbeiter der Debitorenbuchhaltung innerhalb der Finanzabteilung sichtbar ist.

Gut zu wissen:

- Standardmäßig werden neu hinzugefügte Anwendungen in einem Ordner mit dem Namen "Applications" abgelegt. Sie können einen anderen Ordner angeben. Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie den empfohlenen eindeutigen Namen annehmen, wird die Anwendung unter dem Namen hinzugefügt, ansonsten müssen Sie sie umbenennen, damit sie hinzugefügt werden kann. Weitere Informationen finden Sie unter Verwalten von Anwendungsordnern.
- Sie können Anwendungseigenschaften (Einstellungen) beim Hinzufügen oder später ändern. Weitere Informationen finden Sie unter Ändern der Eigenschaften. Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft "Anwendungsname (Benutzer)", sonst wird den Benutzern der Name in Citrix Receiver doppelt angezeigt.
- Wenn Sie eine Anwendung mehreren Anwendungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Anwendungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Gruppen, denen die Anwendung hinzugefügt wurde.

Klicken Sie auf Sie die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

| Quelle | Beschreibung |
|---|---|
| Vom Startmenü | Anwendungen, die auf einer Maschine in den ausgewählten Bereitstellungsgruppen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**.<br><br>Diese Quelle kann nicht ausgewählt werden, wenn Sie (1) Anwendungsgruppen gewählt haben, denen keine Bereitstellungsgruppen zugeordnet sind, (2) Anwendungsgruppen gewählt haben, deren zugeordnete Bereitstellungsgruppen keine Maschinen enthalten, oder (3) eine Bereitstellungsgruppe gewählt haben, die keine Maschinen enthält. |
| Manuell | Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **OK**. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Vorhandene | Anwendungen, die der Site bereits hinzugefügt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**.<br><br>Diese Quelle kann nicht ausgewählt werden, wenn es in der Site keine Anwendungen gibt. |
| App-V | Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Aktivieren Sie dort die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Weitere Informationen finden Sie im Artikel App-V.<br><br>Diese Quelle kann nicht ausgewählt werden (oder wird möglicherweise nicht angezeigt), wenn App-V für die Site nicht konfiguriert ist. |

Wie bereits erwähnt, können Einträge in der Dropdownliste **Hinzufügen** nicht ausgewählt werden, wenn es keine gültige Quelle des jeweiligen Typs gibt. Nicht kompatible Quellen werden nicht aufgelistet (z. B. können Sie Anwendungsgruppen keine Anwendungsgruppen hinzufügen, daher wird diese Quelle nicht angezeigt).

Diese Seite wird nur angezeigt, wenn Sie zuvor einen Geltungsbereich erstellt haben. Standardmäßig ist der Geltungsbereich **Alle** ausgewählt. Weitere Informationen finden Sie im Artikel Delegierte Administration.

Geben Sie einen Namen für die Anwendungsgruppe ein. Sie können optional auch eine Beschreibung eingeben.

Lesen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwalten von Anwendungsgruppen

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Aktivieren und Deaktivieren von Anwendungsgruppen
- Aktivieren und Deaktivieren der Anwendungssitzungsfreigabe zwischen Anwendungsgruppen
- Umbenennen von Anwendungsgruppen
- Hinzufügen und Entfernen von Bereitstellungsgruppenzuordnungen für Anwendungsgruppen und Ändern der Priorität von Gruppenzuordnungen
- Hinzufügen und Entfernen von Benutzern zu bzw. aus Anwendungsgruppen
- Ändern der Geltungsbereiche in Anwendungsgruppen
- Löschen von Anwendungsgruppen


# Einführung

In diesem Abschnitt wird die Verwaltung von Anwendungsgruppen beschrieben, die Sie erstellt haben.

Der Artikel Anwendungen enthält Informationen zur Verwaltung von Anwendungen in Anwendungsgruppen oder Bereitstellungsgruppen. Es werden u. a. folgende Themen behandelt:

- Hinzufügen und Entfernen von Anwendungen zu bzw. aus Anwendungsgruppen
- Ändern der Gruppenzuordnungen einer Anwendung

Zum Verwalten von Anwendungsgruppen sind die Berechtigungen zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Weitere Informationen finden Sie im Artikel Delegierte Administration.

# Aktivieren und Deaktivieren von Anwendungsgruppen

Wenn eine Anwendungsgruppe aktiviert wurde, kann sie die Anwendungen bereitstellen, die ihr hinzugefügt wurden. Durch Deaktivieren einer Anwendungsgruppe werden alle darin enthaltenen Anwendungen deaktiviert. Anwendungen, die auch anderen aktivierten Anwendungsgruppen zugeordnet sind, können über diese Gruppen bereitgestellt werden. Wenn eine Anwendung nicht nur einer Anwendungsgruppe, sondern explizit auch einer mit der Anwendungsgruppe verknüpften Bereitstellungsgruppe hinzugefügt wurde, hat das Deaktivieren der Anwendungsgruppe keine Auswirkungen auf die Anwendung in der Bereitstellungsgruppe.

Anwendungsgruppen werden beim Erstellen aktiviert. Dies können Sie bei der Erstellung nicht ändern.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Anwendungsgruppe aktivieren**.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen und das Fenster geöffnet zu lassen, oder auf **OK**, um die Änderungen zu übernehmen und das Fenster zu schließen.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# Aktivieren und Deaktivieren der Anwendungssitzungsfreigabe zwischen Anwendungsgruppen

Die Sitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen aktiviert. Dies können Sie bei der Erstellung nicht ändern. Weitere Informationen über die Sitzungsfreigabe finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Freigabe von Anwendungssitzungen zwischen Anwendungsgruppen aktivieren**.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen und das Fenster geöffnet zu lassen, oder auf **OK**, um die Änderungen zu übernehmen und das Fenster zu schließen.

# Umbenennen von Anwendungsgruppen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe umbenennen**.
3. Geben Sie einen neuen eindeutigen Namen ein und klicken Sie auf **OK**.

# Hinzufügen und Entfernen von Bereitstellungsgruppenzuordnungen für Anwendungsgruppen und Ändern der Priorität von Gruppenzuordnungen

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, (1) wenn die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren Version von XenDesktop 7.x erstellt wurde, und (2) wenn Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen" geändert, wenn für das Dialogfeld "Anwendungsgruppe bearbeiten" ein Commit ausgeführt wird.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Bereitstellungsgruppen**.
4. Klicken Sie zum Hinzufügen von Bereitstellungsgruppen auf **Hinzufügen**. Aktivieren Sie die Kontrollkästchen verfügbarer Bereitstellungsgruppen. (Nicht kompatible Bereitstellungsgruppen können nicht ausgewählt werden.) Wenn Sie fertig sind, klicken Sie auf **OK**.
5. Zum Entfernen von Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen der jeweiligen Gruppen und klicken Sie auf **Entfernen**. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.
6. Zum Ändern der Priorität von Bereitstellungsgruppen, wählen Sie das Kontrollkästchen einer Bereitstellungsgruppe und klicken Sie auf **Priorität bearbeiten**. Geben Sie die Priorität an (0=höchste) und klicken Sie auf **OK**.
7. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen und das Fenster geöffnet zu lassen, oder auf **OK**, um die Änderungen zu übernehmen und das Fenster zu schließen.

# Hinzufügen und Entfernen von Benutzern zu bzw. aus Anwendungsgruppen

Ausführliche Informationen zu Benutzern finden Sie im Abschnitt "Benutzer" des Artikels Erstellen von Anwendungsgruppen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Benutzer**. Geben Sie an, ob alle Benutzer oder nur bestimmte Benutzer und Gruppen in den zugeordneten Bereitstellungsgruppen Anwendungen in der Anwendungsgruppe verwenden können sollen. Zum Hinzufügen von Benutzern klicken Sie auf **Hinzufügen** und geben Sie die gewünschten Benutzer an. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und klicken Sie auf **Entfernen**.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen und das Fenster geöffnet zu lassen, oder auf **OK**, um die Änderungen zu übernehmen und das Fenster zu schließen.

# Ändern der Geltungsbereiche in Anwendungsgruppen

Sie können Geltungsbereiche nur dann ändern, wenn Sie einen Geltungsbereich erstellt haben. Den Geltungsbereich "Alle" können Sie nicht bearbeiten. Weitere Informationen finden Sie im Artikel Delegierte Administration.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Geltungsbereiche**. Aktivieren oder deaktivieren Sie das Kontrollkästchen neben einem Geltungsbereich.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen und das Fenster geöffnet zu lassen, oder auf **OK**, um die Änderungen zu übernehmen und das Fenster zu schließen.

# Löschen von Anwendungsgruppen

Eine Anwendung muss mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Wenn durch das


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Löschen einer Anwendungsgruppe eine oder mehrere Anwendungen nicht mehr zu einer Gruppe gehören würden, wird eine Warnung angezeigt, dass mit dem Löschen der Gruppe auch diese Anwendungen gelöscht würden. Sie können den Löschvorgang dann bestätigen oder abbrechen.

Durch das Löschen einer Anwendung wird diese nicht aus der ursprünglichen Quelle gelöscht, doch wenn Sie sie wieder zur Verfügung stellen möchten, müssen Sie sie erneut hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Gruppe löschen**.
3. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Remote-PC-Zugriff

Jul 08, 2016

Mit Remote-PC-Zugriff kann ein Endbenutzer sich remote von jedem Standort aus an einem physischen Windows-PC im Büro anmelden.

> **Important**
>
> Verwenden Sie die Befehlszeile in XenApp und XenDesktop 7.9 nur für Remote-PC-Zugriff-Bereitstellungen. Weitere Informationen finden Sie unter Installieren an der Befehlszeile und Bekannte Probleme [#637741].

Der Virtual Delivery Agent (VDA) wird auf dem Büro-PC installiert. Er registriert sich bei dem Delivery Controller und verwaltet die HDX-Verbindung zwischen dem PC und den Clientgeräten des Endbenutzers. Remote-PC-Zugriff unterstützt ein Self-Service Modell. Nach der Einrichtung der Positivliste der Maschinen, die für Benutzer zugänglich sind, können die entsprechenden Benutzer ihre Büro-PCs einer Site ohne Eingriff des Administrators hinzufügen. Citrix Receiver wird auf ihrem Clientgerät ausgeführt und ermöglicht Zugriff auf alle Anwendungen und Daten auf dem Büro-PC von der Remote-PC-Zugriff-Desktopsitzung aus.

Ein Benutzer kann mehrere Desktops haben, einschließlich mehrere physische PCs oder eine Kombination von physischen PCs und virtuellen Desktops.

**Hinweis:** Energiesparmodus und Ruhezustand werden für Remote-PC-Zugriff nicht unterstützt. Remote-PC-Zugriff gilt nur für XenDesktop-Lizenzen. Sitzungen verbrauchen Lizenzen genauso wie andere XenDesktop-Sitzungen.

# Überlegungen zu Active Directory

Bevor Sie die Bereitstellungssite für Remote-PC-Zugriff konfigurieren, richten Sie die Organisationseinheiten und Sicherheitsgruppen ein und erstellen Sie dann Benutzerkonten. Verwenden Sie diese Konten, um die Benutzer für die Bereitstellungsgruppen anzugeben, die für Remote-PC-Zugriff verwendet werden.

Wenn Sie Active Directory modifizieren, nachdem eine Maschine dem Maschinenkatalog hinzugefügt wurde, wird diese Zuweisung von Remote-PC-Zugriff nicht erneut ausgewertet. Sie können, falls erforderlich, Maschinen manuell einem anderen Katalog zuweisen.

Wenn Sie Organisationseinheiten verschieben oder löschen, sind die für Remote-PC-Zugriff verwendeten möglicherweise nicht mehr aktuell. VDAs sind u. U. (wenn überhaupt) nicht mehr dem am besten geeigneten Maschinenkatalog bzw. der am besten geeigneten Bereitstellungsgruppe zugewiesen.

# Überlegungen zu Maschinenkatalogen und Bereitstellungsgruppen

Eine Maschine kann nur jeweils einem Maschinenkatalog und einer Bereitstellungsgruppe zugewiesen sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sie können Maschinen in einen oder mehrere Remote PC-Zugriff-Maschinenkataloge einfügen.

Wenn Sie Maschinenkonten für den Maschinenkatalog auswählen, wählen Sie die niedrigste zutreffende Organisationseinheit, um einen möglichen Konflikt mit Maschinen eines anderen Maschinenkatalogs zu vermeiden. Beispiel: Im Fall von Bank/Bankbeamte/Kassierer, wählen Sie Kassierer.

Sie können alle Maschinen eines Remote-PC-Zugriff-Maschinenkatalogs über eine oder mehrere Bereitstellungsgruppen zuweisen. Wenn eine Benutzergruppe beispielsweise bestimmte Richtlinieneinstellungen und eine andere Gruppe andere Einstellungen benötigt, können Sie die Benutzer unterschiedlichen Bereitstellungsgruppen zuweisen und so die HDX-Richtlinien nach Bereitstellungsgruppe filtern.

Wenn die Benutzerbetreuung in Ihrer IT-Infrastruktur auf dem geografischen Standort, der Abteilung oder einer anderen Kategorie beruht, können Sie Maschinen und Benutzer entsprechend gruppieren und so die delegierte Administration ermöglichen. Stellen Sie sicher, dass jeder Administrator über Berechtigungen für die relevanten Maschinenkataloge und die entsprechenden Bereitstellungsgruppen hat.

Erstellen Sie für Benutzer mit Büro-PCs mit Windows XP einen separaten Maschinenkatalog und eine separate Bereitstellungsgruppe für diese Systeme. Aktivieren Sie bei der Auswahl von Maschinenkonten für diesen Katalog in Studio das Kontrollkästchen für Maschinen, die unter Windows XP ausgeführt werden.

# Überlegungen zur Bereitstellung

Sie können eine Remote-PC-Zugriff-Bereitstellung erstellen und dann später konventionelle Virtual Desktop Infrastructure-Desktops (VDI) oder Anwendungen hinzufügen. Sie können auch Remote-PC-Zugriff-Desktops einer vorhandenen VDI-Bereitstellung hinzufügen.

Erwägen Sie eine Aktivierung der Microsoft-Remoteunterstützung bei der VDA-Installation auf Büro-PCs. Diese Option ermöglicht es den Helpdeskteams, die Director verwenden, Benutzersitzungen mit der Microsoft-Remoteunterstützung anzuzeigen und zu steuern.

Legen Sie fest, wie Sie den VDA auf jedem Büro-PC bereitstellen möchten. Citrix empfiehlt, eine elektronische Softwareverteilung zu verwenden, z. B. Active Directory-Skripts und Microsoft System Center Configuration Manager. Das Installationsmedium enthält Active Directory-Beispielskripts.

Lesen Sie für Remote-PC-Zugriff-Bereitstellungen den Artikel Sicherheitsüberlegungen.

Sicherer Start für Remote-PC-Zugriff wird zurzeit auf Windows 10 und 8.1 unterstützt. Deaktivieren Sie sicheren Start, wenn Sie den Workstation-VDA auf anderen Betriebssystemen bereitstellen.

Jeder Büro-PC muss in der Domäne per Netzwerkkabel verbunden sein.

Windows 7 Aero wird für Büro-PCs unterstützt, ist aber nicht erforderlich.

Tastatur und Maus müssen direkt am PC oder Laptop angeschlossen werden, nicht am Bildschirm oder an anderen Komponenten, die ausgeschaltet werden können. Wenn Sie Eingabegeräte an solche Komponenten (z. B. Bildschirme) anschließen müssen, sollten diese nicht ausgeschaltet werden.

Wenn Sie Smartcards verwenden, lesen Sie den Artikel Smartcards.

Remote-PC-Zugriff kann auf den meisten Laptop-Computern verwendet werden. Für einen besseren Zugriff und die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

optimale Verbindung konfigurieren Sie die Energiesparoptionen bei Laptops wie die eines Desktop-PCs. Beispiel:

- Deaktivieren Sie den Ruhezustand.
- Deaktivieren Sie den Standbymodus.
- Legen Sie die Aktion beim Schließen des Deckels auf "Keine Aktion" fest.
- Legen Sie die Aktion bei Betätigen der Ein-/Ausschalttaste auf "Herunterfahren" fest.
- Deaktivieren Sie die Energiesparfunktionen der Grafikkarte.
- Deaktivieren Sie die Energiesparfunktionen der Netzwerkkarte.
- Deaktivieren Sie Akku-Energiespartechnologien.

Folgendes wird für Remote-PC-Zugriff-Geräte nicht unterstützt:

- An-/Ausdocken des Laptops.
- KVM-Switches oder andere Komponenten, die eine Sitzung trennen.
- Hybrid-PCs, einschließlich All-in-One- und NVIDIA Optimus-Laptops und -PCs.

Remote-PC-Zugriff kann auf den meisten Surface Pro-Geräten verwendet werden. XenDesktop 7.9 unterstützt Remote-PC-Zugriff auf Surface Pro-Geräten mit Windows 8.1 oder 10. Für einen besseren Zugriff und die optimale Verbindung konfigurieren Sie das Surface-Gerät wie einen Desktop-PC oder einen Laptop. Beispiel:

- Deaktivieren Sie den Standbymodus oder den Ruhezustand.
- Verwenden Sie eine Kabelnetzwerkverbindung.
- Die Tastatur sollte immer angeschlossen sein, wenn Sie eine Sitzung initiieren oder wiederverbinden.
- Deaktivieren Sie Akku-Energiespartechnologien.

Installieren Sie Citrix Receiver auf jedem Clientgerät mit Remotezugriff auf den Büro-PC.

Mehrere Benutzer mit Remotezugriff auf denselben Büro-PC sehen in Citrix Receiver dasselbe Symbol. Wenn ein Benutzer eine Remoteanmeldung am PC vornimmt, wird diese Ressource anderen Benutzern als nicht verfügbar angezeigt.

Standardmäßig wird eine Remotesitzung des Benutzers automatisch getrennt, wenn ein lokaler Benutzer eine Sitzung auf dieser Maschine (durch Drücken von Strg + Alt + Entf) initiiert. Fügen Sie den folgenden Registrierungseintrag auf dem Büro-PC hinzu und starten Sie dann die Maschine neu, um diese automatische Aktion zu verhindern.

> **Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.
>
> HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001
>
> Zur weiteren Anpassung des Verhaltens dieses Features: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC
>
> RpcaMode (dword):
>
> > 1 = Remotebenutzer gewinnt immer, wenn er nicht innerhalb des angegebenen Timeouts auf die Meldung reagiert.
> >
> > 2 = Lokaler Benutzer gewinnt immer. Wenn diese Einstellung nicht festgelegt wird, gewinnt standardmäßig der Remotebenutzer.
>
> RpcaTimeout (dword):
>
> > Timeout in Sekunden für den Benutzer, bis entschieden wird, welche Art von Modus erzwungen werden soll. Wenn diese Einstellung nicht festgelegt wird, gilt der Standardwert von 30 Sekunden. Als Mindestwert sollte hier 30 Sekunden festgelegt werden. Der Benutzer muss den Computer neu starten, damit die Änderungen in Kraft treten.
> >
> > Wenn der lokale Benutzer den Zugriff auf die Konsole erzwingen möchte, kann er innerhalb von 10 Sekunden zwei Mal Strg + Alt + Entf drücken, um

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

lokal auf die Remotesitzung zuzugreifen und eine Verbindungstrennung zu erzwingen.

Wenn ein lokaler Benutzer nach der Registrierungsänderung und dem Maschinenneustart für die Anmeldung am PC Strg+Alt+Entf drückt und der Computer von einem Remotebenutzer verwendet wird, wird der Remotebenutzer gefragt, ob er die Verbindung des lokalen Benutzers zulässt oder verweigert. Bei der Zulassung der Verbindung wird die Sitzung des Remotebenutzers getrennt.

### Remote-PC-Zugriff und HDX 3D Pro-Modus

Für Remote-PC-Zugriff ist der VDA normalerweise mit der standardmäßigen VDA-Option konfiguriert. Für Remote-PC-Zugriff, der mit HDX 3D Pro konfiguriert ist, wird das Ausblenden des Bildschirms für Intel Iris Pro Graphics und Intel HD Graphics 5300 und höher unterstützt (Intel Core-Prozessoren der 5. Generation und Intel Core i5-Prozessoren der 6. Generation) sowie für NVIDIA Quadro- und NVIDIA GRID-GPUs.

Weitere Informationen finden Sie unter Vorbereiten der Installation und GPU-Beschleunigung für Windows-Desktopbetriebssysteme.

# Wake-On-LAN

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden, z. B. bei witterungsbedingten Problemen.

Das Wake-On-LAN-Feature von Remote-PC-Zugriff wird auf Folgendem unterstützt:

- PCs, die Intel Active Management Technology (AMT) unterstützen.
- PCs, auf denen Wake-On-LAN im BIOS aktiviert ist.

Sie müssen Microsoft System Center Configuration Manager (ConfigMgr) 2012 konfigurieren, um das Wake-On-LAN-Feature zu verwenden. ConfigMgr bietet Zugriff auf AMT-Energiebefehle für den Computer und Unterstützung für den Aktivierungsproxy sowie Magic Packets. Wenn Sie anschließend mit Studio eine Bereitstellung für den Remote-PC-Zugriff erstellen (bzw. wenn Sie eine andere Energieverwaltungsverbindung für den Remote-PC-Zugriff hinzufügen), aktivieren Sie die Energieverwaltung und geben Sie ConfigMgr-Zugriffsinformationen an.

Beachten Sie außerdem Folgendes:

- Die Verwendung der AMT-Energieverwaltung wird aus Gründen der Sicherheit und Sitzungszuverlässigkeit zwar bevorzugt, es werden jedoch auch zwei Methoden ohne AMT unterstützt: ConfigMgr-Aktivierungsproxy und Magic Packets.
- Nur AMT-fähige Maschinen: Das Wake-On-LAN-Feature unterstützt auch die Aktionen "Herunterfahren erzwingen" und "Neustart erzwingen" von Studio und Director. Außerdem ist in StoreFront und Receiver eine Neustartaktion verfügbar.

Weitere Informationen finden Sie unter Microsoft System Center Configuration Manager und Remote-PC-Zugriff-Wake-On-LAN.

Weitere Informationen zum Wake-On-LAN-SDK, das im Rahmen einer Machbarkeitsstudie zur Verfügung gestellt wird und mit dem Sie oder der Drittanbieter einer Wake-On-LAN-Lösung ohne System Center 2012 R2 einen Connector erstellen können, finden Sie unter CTX202272. Das Wake-On-LAN-SDK in diesem Release ist nur für Evaluierungszwecke vorgesehen und nicht für die Verwendung in einer Produktionsumgebung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurationsreihenfolge und Überlegungen

### Vor Erstellen der Remote-PC-Zugriff-Site

Wenn Sie das Energieverwaltungsfeature von Remote-PC-Zugriff ("Remote-PC-Zugriff-Wake-On-LAN") verwenden möchten, führen Sie die Konfigurationsaufgaben auf den PCs und in Microsoft System Center Configuration Manager (ConfigMgr) vor dem Erstellen der Remote-PC-Zugriff-Bereitstellung in Studio durch. Weitere Informationen finden Sie unter Microsoft System Center Configuration Manager und Remote-PC-Zugriff-Wake-On-LAN.

### Im Assistenten für die Siteerstellung

- Wählen Sie als Sitetyp "Remote-PC-Zugriff-Site".
- Auf der Seite "Energieverwaltung" können Sie die Energieverwaltung für die Maschinen im Standardmaschinenkatalog für Remote-PC-Zugriff aktivieren oder deaktivieren. Wenn Sie die Energieverwaltung aktivieren, geben Sie ConfigMgr-Verbindungsinformationen an.
- Geben Sie auf den Seiten "Benutzer" und "Maschinenkonten" Benutzer und Maschinenkonten an.

Bei der Erstellung einer Remote-PC-Zugriff-Site werden ein Standardmaschinenkatalog unter dem Namen "Remote-PC-Zugriff-Maschinen" und eine Standardbereitstellungsgruppe unter dem Namen "Remote-PC-Zugriff-Desktops" erstellt.

### Wenn Sie einen weiteren Maschinenkatalog für die Verwendung mit Remote-PC-Zugriff erstellen, gilt Folgendes:

- Wählen Sie auf der Seite "Betriebssystem" die Option "Remote-PC-Zugriff" und eine Energieverwaltungsverbindung. Das Verwenden der Energieverwaltung ist nicht obligatorisch. Wenn keine Energieverwaltungsverbindungen konfiguriert sind, können Sie nach dem Abschließen des Assistenten für die Erstellung eines Maschinenkatalogs eine erstellen (Verbindungstyp=Microsoft Configuration Manager-Wake-On-LAN) und dann den Maschinenkatalog unter Angabe der neuen Verbindung bearbeiten.
- Auf der Seite "Maschinenkonten" können Sie Maschinenkonten oder Organisationseinheiten auswählen oder hinzufügen.

**Installieren Sie den VDA auf den Büro-PCs, die für lokalen und Remotezugriff verwendet werden.** Normalerweise wird der VDA automatisch mit dem Verwaltungssoftwarepaket bereitgestellt. Bei Test- oder kleinen Bereitstellungen können Sie jedoch den VDA manuell auf jedem Büro-PC installieren.

Wenn Sie den VDA über die Befehlszeile installieren, schließen Sie die Option **/remotepc** ein. Dadurch wird die Installation der folgenden Komponenten auf einem Desktopbetriebssystem (Workstation) verhindert:

- App V-Komponente: Citrix Personalisierung für App-V - VDA
- UpmComponent: Citrix User Profile Manager
- UpmVdaPlugin-Komponente: Citrix User Profile Manager WMI-Plug-In
- Mps Component: Maschinenidentitätsdienst
- VDisk-Komponente: Personal vDisk

Wenn diese Komponenten während eines Upgrades installiert werden, werden sie vom Installationsprogramm erkannt und aktualisiert.

Wenn der VDA installiert ist, wird der nächste Domänenbenutzer, der sich auf dem Büro-PC bei einer Konsolensitzung anmeldet (lokal oder über RDP), automatisch dem Remote-PC-Zugriff-Desktop zugewiesen. Wenn in der Konsolensitzung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

weitere Domänenbenutzer angemeldet werden, werden sie der Desktopbenutzerliste unter Berücksichtigung der eingerichteten Beschränkungen ebenfalls hinzugefügt.

Zum Verwenden von RDP-Verbindungen außerhalb Ihrer XenApp- bzw. XenDesktop-Umgebung müssen Sie Benutzer oder Gruppen zur Gruppe der Benutzer mit direktem Zugriff hinzufügen.

**Weisen Sie die Benutzer an, auf jedem Clientgerät, das sie für den Remotezugriff auf den Büro-PC verwenden, Citrix Receiver herunterzuladen und zu installieren.** Citrix Receiver ist unter http://www.citrix.com oder in den Anwendungsverteilungssystemen für unterstützte Mobilgeräte verfügbar.

# Konfigurieren erweiterter Verbindungseinstellungen

Sie können eine Energieverwaltungsverbindung zum Konfigurieren der erweiterten Einstellungen bearbeiten. Sie können Folgendes aktivieren:

- ConfigMgr-Aktivierungsproxy
- Wake-On-LAN-Pakete (Magic Packets). Wenn Sie Wake-On-LAN-Pakete aktivieren, können Sie eine Wake-On-LAN-Übertragungsmethode auswählen: subnetzgesteuertes Broadcast oder Unicast.

Der PC verwendet AMT-Energiebefehle (sofern unterstützt) und alle aktivierten erweiterten Einstellungen. Wenn der PC keine AMT-Befehle verwendet, werden die erweiterten Einstellungen verwendet.

# Problembehandlung

Der Delivery Controller schreibt die folgenden Diagnoseinformationen über Remote-PC-Zugriff in das Windows-Anwendungsereignisprotokoll. Informationsmeldungen werden nicht eingeschränkt. Fehlermeldungen werden durch Löschen doppelter Nachrichten eingeschränkt.

- 3300 (Informationsmeldung): Maschine zum Katalog hinzugefügt
- 3301 (Informationsmeldung): Maschine der Bereitstellungsgruppe hinzugefügt
- 3302 (Informationsmeldung): Maschine dem Benutzer zugewiesen
- 3303 (Fehler): Ausnahme

Wenn die Energieverwaltung für Remote-PC-Zugriff aktiviert ist, können Maschinen, die sich in einem anderen Subnetz als der Controller befinden, ggf. nicht per subnetzgesteuertes Broadcast gestartet werden. Wenn Sie eine subnetzübergreifende Energieverwaltung mit subnetzgesteuertem Broadcast benötigen und AMT nicht unterstützt wird, versuchen Sie es mit dem Aktivierungsproxy oder Unicast (stellen Sie sicher, dass diese Einstellungen in den erweiterten Eigenschaften der Energieverwaltungsverbindung aktiviert sind).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# App-V

Jul 08, 2016

# Verwenden von App-V in XenApp und XenDesktop

Mit Microsoft Application Virtualization (App-V) können Sie Anwendungen als Dienste bereitstellen, aktualisieren und unterstützen. Benutzer können auf Anwendungen zugreifen, ohne sie auf ihren Geräten installieren zu müssen. App-V und Microsoft User State Virtualization (USV) ermöglichen den Zugriff auf Anwendungen und Daten unabhängig vom Standort oder von der Internetverbindung.

Die folgende Tabelle enthält eine Liste der unterstützen Versionen.

| App-V | XenDesktop-/XenApp-Version | |
|---|---|---|
| | Delivery Controller | VDA |
| 5.0 oder 5.0 SP1 | XenDesktop 7 bis aktuelle Version<br>XenApp 7,5 bis aktuelle Version | 7.0 bis aktuelle Version |
| 5.0 SP2 | XenDesktop 7 bis aktuelle Version<br>XenApp 7,5 bis aktuelle Version | 7.1 bis aktuelle Version |
| 5.0 SP3 und 5.1 | XenDesktop 7.6 bis aktuelle Version<br>XenApp 7.6 bis aktuelle Version | 7.6.300 bis aktuelle Version |

Der Offlinezugriff auf Anwendungen wird von App-V-Client nicht unterstützt. Die Unterstützung der App-V-Integration umfasst die Verwendung von SMB-Freigaben für Anwendungen. Das HTTP-Protokoll wird nicht unterstützt.

Wenn Sie mit App-V nicht vertraut sind, konsultieren Sie die Dokumentation von Microsoft. In diesem Artikel werden folgende App-V-Komponenten behandelt:

- **Verwaltungsserver**: bietet eine zentrale Konsole zum Verwalten der App-V-Infrastruktur und stellt virtuelle Anwendungen für den App-V-Desktopclient und den Remotedesktopdienste-Client bereit. Der App-V-Verwaltungsserver führt das vom Administrator benötigte Authentifizieren, Anfordern und Bereitstellen von Sicherheit, Messungen, Überwachung und Sammeln von Daten durch. Der Server verwendet Active Directory und unterstützende Tools zum Verwalten von Benutzern und Anwendungen.
- **Veröffentlichungsserver**: stellt App-V-Clients mit Anwendungen für bestimmte Benutzer bereit und hostet das virtuelle Anwendungspaket für das Streaming. Die Pakete werden vom Verwaltungsserver abgerufen.
- **Client**: ruft virtuelle Anwendungen ab, veröffentlicht die Anwendungen auf dem Client und erstellt und verwaltet automatisch virtuelle Umgebungen zur Laufzeit auf Windows-Geräten. Der App-V-Client wird auf dem VDA installiert und


© 1999-2017 Citrix Systems, Inc. All rights reserved.

speichert dort in jedem Benutzerprofil benutzerspezifische Einstellungen für virtuelle Anwendungen, z. B. Registrierungs- und Dateiänderungen.

Anwendungen sind nahtlos verfügbar, ohne dass Vorkonfigurationen oder Änderungen an den Einstellungen des Betriebssystems vorgenommen werden müssen. Sie können App-V-Anwendungen von Serverbetriebssystem- und Desktopbetriebssystem-Bereitstellungsgruppen starten:

- Über Citrix Receiver
- Vom Startmenü
- Über den App-V-Client und Citrix Receiver
- Gleichzeitig von mehreren Benutzern auf mehreren Geräten
- Über Citrix StoreFront

Geänderte App-V-Anwendungseigenschaften werden implementiert, wenn die Anwendung gestartet wird. Beispiel: Bei Anwendungen mit einem geänderten Anzeigenamen oder einem angepassten Symbol wird die Modifikation angezeigt, wenn Benutzer die Anwendung starten.

Sie können mit dem App-V Sequencer erstellte und auf einem App-V-Server oder einer Netzwerkfreigabe gehostete App-V-Pakete verwenden.

- **App-V-Server**: Die Verwendung von Anwendungen aus Paketen auf App-V-Servern erfordert eine ständige Verbindung zwischen Studio und App-V-Server für Ermittlung, Konfiguration und Download auf die VDAs. Die ist mit Hardware-, Infrastruktur- und Verwaltungsaufwand verbunden. Studio und App-V-Server müssen insbesondere für die Benutzerberechtigungen immer synchronisiert bleiben.

  Diese Methode wird als *duale Verwaltung* bezeichnet, da der Zugriff auf App-V-Pakete und -Anwendungen sowohl die Studio- als auch die App-V-Serverkonsole erfordert. Die Methode funktioniert besten in gekoppelten App-V-/Citrix Bereitstellungen.

- **Netzwerkfreigabe**: Werden Pakete in Netzwerkfreigaben gespeichert, ist Studio nicht von der App-V-Server- und Datenbankinfrastruktur abhängig, wodurch sich der entsprechende Aufwand verringert. (Sie müssen den Microsoft App-V-Client auf jedem VDA installieren.)

  Diese Methode wird als *Einzelverwaltung* bezeichnet, da die Verwendung von App-V-Paketen und -Anwendungen nur die Studiokonsole erfordert. Sie navigieren zu der Netzwerkfreigabe und fügen App-V-Pakete von dort der Anwendungsbibliothek auf Siteebene hinzu.

  Mit dem Citrix Begriff "Anwendungsbibliothek" wird das Repository zur Zwischenspeicherung von Informationen über App-V-Pakete bezeichnet. In der Anwendungsbibliothek werden auch Informationen für andere Citrix Technologien zur Anwendungsbereitstellung gespeichert.

Sie können eine Verwaltungsmethode verwenden oder beide parallel. Das heißt, wenn Sie Bereitstellungsgruppen Anwendungen hinzufügen, dürfen diese aus App-V-Paketen auf App-V-Servern und/oder in einer Netzwerkfreigabe stammen.

Wenn Sie **Konfiguration > App-V-Veröffentlichung** im Navigationsbereich von Studio wählen, werden App-V-Paketnamen und -quellen angezeigt. In der Spalte "Quelle" wird angegeben, ob die Pakete auf dem App-V-Server oder in der Anwendungsbibliothek gespeichert sind. Wenn Sie ein Paket auswählen, werden im Detailbereich die Anwendungen im Paket angezeigt.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

# Einrichtung

Die folgende Tabelle enthält die Reihenfolge der Setupaufgaben zur Verwendung von App-V in XenApp und XenDesktop.

| Verwaltungsmethode | | Aufgabe |
|---|---|---|
| Einzelverwaltung | Duale Verwaltung | |
| X | X | Bereitstellen von App-V |
| X | X | Bereitstellen von Paketen |
| | X | Konfigurieren von App-V-Serveradressen in Studio |
| X | X | Installieren von Software auf VDA-Maschinen |
| X | | Hinzufügen von App-V-Paketen zur Anwendungsbibliothek |
| X | X | Hinzufügen von App-V-Anwendungen zu Bereitstellungsgruppen |

Anweisungen zur App-V-Bereitstellung finden Sie unter http://technet.microsoft.com/en-us/virtualization/hh710199.

Optional können Sie die Einstellungen des App-V-Veröffentlichungsservers ändern. Citrix empfiehlt die Verwendung der SDK-Cmdlets auf dem Controller. Einzelheiten finden Sie in der SDK-Dokumentation.

- Zum Anzeigen der Einstellungen des Veröffentlichungsservers geben Sie **Get-CtxAppvServerSetting -AppVPublishingServer <*Veröffentlichungsserver*>** ein.
- Um sicherzustellen, dass App-V-Anwendungen richtig gestartet werden, geben Sie **Set-CtxAppvServerSetting –UserRefreshonLogon 0** ein.

Wenn Sie zuvor GPO-Richtlinieneinstellungen für die Verwaltung der Veröffentlichungsservereinstellungen verwendet haben, werden die App-V-Integrationseinstellungen einschließlich Cmdlet-Einstellungen von den GPO-Einstellungen außer Kraft gesetzt. Dies kann dazu führen, dass der Start von App-V-Anwendungen fehlschlägt. Citrix empfiehlt, dass Sie alle GPO-Richtlinieneinstellungen entfernen und diese Einstellungen dann mit dem SDK konfigurieren.

Erstellen Sie bei beiden Verwaltungsmethoden Anwendungspakete mit dem App-V Sequencer. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation.

- Für die Einzelverwaltung stellen Sie die Pakete an einem freigegebenen UNC- oder SMB-Speicherort im Netzwerk zur Verfügung. Stellen Sie sicher, dass der Studio-Administrator, der den Bereitstellungsgruppen Anwendungen hinzufügt,


© 1999-2017 Citrix Systems, Inc. All rights reserved.

zumindest Lesezugriff auf diesen Speicherort hat.
- Für die duale Verwaltung veröffentlichen Sie die Pakete auf dem App-V-Verwaltungsserver.

Unabhängig davon, ob die Pakete auf dem App-V-Server oder in einer Netzwerkfreigabe sind, stellen Sie sicher, dass ihre Sicherheitsberechtigungen den Zugriff durch den Studio-Administrator gestatten.

Diese Vorgehensweise gilt nur für die duale Verwaltung.

Geben Sie für die duale Verwaltung die Adressen von App-V-Verwaltungsserver und -Veröffentlichungsserver während oder nach der Erstellung der Site an. Sie können dies während oder nach dem Erstellen der Site tun.

Während der Siteerstellung:

> Geben Sie auf der Seite **App-V** des Assistenten die URL des App-V-Verwaltungsservers und die URL und Portnummer des App-V- Veröffentlichungsservers an. Testen Sie die Verbindung, bevor Sie mit dem Assistenten fortfahren. Wenn der Test fehlschlägt, konsultieren Sie den Abschnitt "Problembehandlung" weiter unten.

Nach der Siteerstellung:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > App-V-Veröffentlichung**.
2. Wenn Sie die App-V-Serveradressen noch nicht angegeben haben, wählen Sie **Microsoft Server hinzufügen** im Aktionsbereich.
3. Zum Ändern der App-V-Serveradressen wählen Sie **Microsoft Server bearbeiten** im Aktionsbereich.
4. Geben Sie die URL für den Microsoft App-V-Verwaltungsserver und die URL und Portnummer des App-V-Veröffentlichungsservers ein.
5. Testen Sie die Verbindung mit diesen Servern, bevor Sie das Dialogfeld schließen. Wenn der Test fehlschlägt, konsultieren Sie den Abschnitt "Problembehandlung" weiter unten.

Wenn Sie später alle Verbindungen mit App-V-Verwaltungsserver und -Veröffentlichungsserver entfernen möchten, damit Studio keine App-V-Pakete auf diesen Servern mehr ermittelt, wählen Sie im Aktionsbereich **Microsoft Server entfernen**. Diese Aktion ist nur zulässig, wenn gerade keine Anwendungen in Paketen auf diesen Servern in einer Bereitstellungsgruppe veröffentlicht sind. Ist dies der Fall, müssen Sie die Anwendungen zuerst von den Bereitstellungsgruppen entfernen, bevor Sie die App-V-Server entfernen können.

Auf Maschinen mit VDAs müssen zur Unterstützung von App-V zwei Softwareanwendungen installiert sein: eine von Microsoft und eine von Citrix.

**Microsoft App-V-Client**

> Diese Anwendung ruft virtuelle Anwendungen ab, veröffentlicht die Anwendungen auf dem Client und erstellt und verwaltet automatisch virtuelle Umgebungen zur Laufzeit auf Windows-Geräten. Der App-V-Client speichert benutzerspezifische virtuelle Anwendungseinstellungen, wie Registrierungs- und Dateiänderungen, in den Benutzerprofilen.
>
> Der App-V-Client ist bei Microsoft erhältlich. Installieren Sie den Client auf jeder Maschine mit einem VDA oder auf dem Masterimage in einem Maschinenkatalog, das zum Erstellen von VMs verwendet wird.
>
> Tipp: Nach der Installation des App-V-Clients mit Administratorberechtigungen führen Sie das PowerShell-Cmdlet **Get-**

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

**AppvClientConfiguration** aus und vergewissern Sie sich, dass "EnablePackageScripts" auf 1 gesetzt ist. Wenn es nicht auf "1" gesetzt ist, führen Sie **Set-AppvClientConfiguration -EnablePackageScripts $true** aus.

Citrix App-V-Komponenten

Die Citrix App-V-Komponentensoftware wird standardmäßig installiert und aktiviert, wenn Sie einen VDA installieren. Dabei wird auch ein Konto mit lokalen Administratorberechtigungen für den Zugriff auf die App-V-Veröffentlichungskomponenten erstellt.

Sie können diese Standardaktion während der Installation steuern. Deaktivieren Sie in der grafischen Oberfläche das Kontrollkästchen **Citrix App-V-Veröffentlichungskomponenten installieren** auf der Seite **Features**. In der Befehlszeilenschnittstelle verwenden Sie die Option **/no_appv**.

Wenn Sie die Citrix App-V-Komponenten bei der VDA-Installation deaktiviert haben und später App-V-Anwendungen verwenden möchten, klicken Sie in der Liste "Programme und Funktionen" der Windows-Maschine mit der rechten Maustaste auf den Eintrag **Citrix Virtual Delivery Agent** und dann auf **Ändern**. Ein Assistent wird gestartet. Aktivieren Sie in dem Assistenten die Option zum Installieren und Aktivieren der App-V-Veröffentlichungskomponenten.

Diese Vorgehensweise gilt nur für die Einzelverwaltung.

Sie müssen mindestens Lesezugriff auf die Netzwerkfreigabe mit den App-V-Paketen haben.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > App-V-Veröffentlichung**.
2. Klicken Sie im Aktionsbereich auf **Pakete hinzufügen**.
3. Navigieren Sie zu der Freigabe mit den App-V-Paketen und wählen Sie ein oder mehrere Pakete aus.
4. Klicken Sie auf **Add**.

Nachfolgend wird das Hinzufügen von App-V-Anwendungen zu Bereitstellungsgruppen behandelt. Detaillierte Informationen zum Erstellen von Bereitstellungsgruppen finden Sie unter Erstellen von Bereitstellungsgruppen.

**Schritt 1:** Wählen Sie aus, ob Sie eine neue Bereitstellungsgruppe erstellen oder App-V-Anwendungen zu einer vorhandenen Bereitstellungsgruppe hinzufügen möchten:

Bereitstellungsgruppe für App-V-Anwendungen erstellen:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie im Aktionsbereich **Bereitstellungsgruppe erstellen** aus.
3. Geben Sie auf den Seiten des Assistenten einen Maschinenkatalog und Benutzer an.

App-V-Anwendungen einer vorhandenen Bereitstellungsgruppe hinzufügen:

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Klicken Sie im Aktionsbereich auf **Anwendungen hinzufügen**.
3. Wählen Sie eine oder mehrere Bereitstellungsgruppen für die App-V-Anwendungen.

**Schritt 2:** Klicken Sie auf der Seite **Anwendungen** des Assistenten auf die Dropdownliste **Hinzufügen**, um Anwendungsquellen anzuzeigen. Wählen Sie **App-V**.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

**Schritt 3:** Wählen Sie auf der Seite **App-V-Anwendungen hinzufügen** als App-V-Quelle entweder den App-V-Server oder die Anwendungsbibliothek. Es werden nun die Anwendungsnamen mit den Paketnamen und -versionen angezeigt. Aktivieren Sie die Kontrollkästchen neben den gewünschten Anwendungen. Klicken Sie dann auf **OK**.

**Schritt 4:** Schließen Sie den Assistenten ab.

Gut zu wissen:

- Wenn Sie beim Hinzufügen einer App-V-Anwendung zu einer Bereitstellungsgruppe die Eigenschaften der Anwendung ändern, treten die Änderungen beim Starten der Anwendung in Kraft. Wenn Sie beispielsweise den Anzeigenamen oder das Symbol einer Anwendung ändern, erscheinen die geänderten Elemente, wenn ein Benutzer die Anwendung startet.
- Wenn Sie später den Bereitstellungstyp einer Bereitstellungsgruppe mit App-V-Anwendungen von "Desktops und Anwendungen" auf "Anwendungen" ändern, ändert sich die Leistung der App-V-Anwendungen nicht.

# Entfernen von App-V-Paketen aus der Anwendungsbibliothek

Beim Entfernen eines App-V-Pakets aus der Anwendungsbibliothek wird es aus dem App-V-Veröffentlichungsknoten in Studio entfernt, die enthaltenen Anwendungen verbleiben jedoch in den Bereitstellungsgruppen und können weiterhin gestartet werden. Das Paket verbleibt an dem Speicherort im Netzwerk. (Dies unterscheidet sich vom Entfernen einer App-V-Anwendung aus einer Bereitstellungsgruppe.)

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration** > **App-V-Veröffentlichung**.
2. Wählen Sie ein oder mehrere Pakete zum Entfernen aus.
3. Wählen Sie im Aktionsbereich **Paket entfernen**.

# Problembehandlung

Probleme, die nur bei Verwendung der dualen Verwaltung auftreten können, sind mit "(DUAL)" gekennzeichnet.

(DUAL) Wenn Sie App-V-Serveradressen in Studio angeben tritt beim Testen der Verbindung ein Fehler auf.

- Wurde der App-V-Server hochgefahren? Senden Sie entweder einen Ping-Befehl oder prüfen Sie die IIS-Verwaltung. Jeder App-V-Server muss den Zustand "Gestartet" und "Ausgeführt" haben.
- Ist auf dem App-V-Server PowerShell-Remoting aktiviert? Ist dies nicht der Fall, konsultieren Sie den Artikel http://technet.microsoft.com/en-us/magazine/ff700227.aspx
- Ist der Studio-Administrator gleichzeitig App-V-Serveradministrator?
- Ist auf dem App-V-Server die Dateifreigabe aktiviert? Geben Sie in Windows Explorer oder über den Befehl "Ausführen" **\\<*App-V-Server-FQDN*>** ein.
- Hat der App-V-Server dieselben Dateifreigabeberechtigungen wie der App-V-Administrator? Fügen Sie auf dem App-V-Server für \\<*App-V-Server-FQDN*> unter "Gespeicherte Benutzernamen und Kennwörter" einen Eintrag mit den Anmeldeinformationen des Benutzers ein, der Administratorberechtigungen auf dem App-V-Server hat. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/306541.
- Ist der App-V-Server in Active Directory?

  Sind Studio-Maschine und App-V-Server in verschiedenen Active Directory-Domänen, zwischen denen keine

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Vertrauensbeziehung besteht, führen Sie über die PowerShell-Konsole auf der Studio-Maschine **winrm s winrm/Config/client '@(TrustedHosts="<*App-V-Server-FQDN*>")'** aus.

Wird "TrustedHosts" über das Gruppenrichtlinienobjekt verwaltet, wird eine Fehlermeldung angezeigt, die besagt, dass die Konfigurationseinstellung "TrustedHosts" nicht geändert werden kann, da sie von Richtlinien gesteuert wird, und dass die Richtlinie auf "Nicht konfiguriert" festgelegt werden müsste, damit die Konfigurationseinstellung geändert werden kann. In diesem Fall fügen Sie einen Eintrag für den App-V-Servernamen in der TrustedHosts-Richtlinie im Gruppenrichtlinienobjekt hinzu (Administrative Vorlagen > Windows-Komponenten > Windows-Remoteverwaltung (WinRM) > WinRM-Client).

(DUAL) Die Ermittlung schlägt beim Hinzufügen einer App-V-Anwendung zu einer Bereitstellungsgruppe fehl.

- Ist der Studio-Administrator gleichzeitig Administrator des App-V-Verwaltungsservers?
- Wird der App-V-Verwaltungsserver ausgeführt? Senden Sie entweder einen Ping-Befehl oder prüfen Sie die IIS-Verwaltung. Jeder App-V-Server muss den Zustand "Gestartet" und "Ausgeführt" haben.
- Ist PowerShell-Remoting auf beiden App-V-Servern aktiviert? Ist dies nicht der Fall, konsultieren Sie den Artikel http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- Haben die Pakete die richtigen Sicherheitsberechtigungen, sodass der Studio-Administrator Zugriff hat?

App-V-Anwendungen werden nicht gestartet.

- (DUAL) Wird der Veröffentlichungsserver ausgeführt?
- (DUAL) Haben die App-V-Pakete die richtigen Sicherheitsberechtigungen, sodass Benutzer Zugriff haben?
- (DUAL) Stellen Sie auf dem VDA sicher, dass "Temp" auf den richtigen Speicherort verweist und dass genügend Speicherplatz im Verzeichnis "Temp" ist.
- (DUAL) Führen Sie auf dem App-V-Veröffentlichungsserver **Get-AppvPublishingServer *** aus, um die Liste der Veröffentlichungsserver anzuzeigen.
- (DUAL) Prüfen Sie auf dem App-V-Veröffentlichungsserver, ob "UserRefreshonLogon" auf "False" festgelegt ist. Sonst schlägt der Start der ersten App-V-Anwendung normalerweise fehl.
- (DUAL) Führen Sie auf dem App-V-Veröffentlichungsserver **Set-AppvPublishingServer** als Administrator aus und legen Sie für "UserRefreshonLogon" "False" fest.
- Ist auf der Maschine mit dem VDA eine unterstützte Version des App-V-Clients installiert? Ist auf dem VDA die Einstellung "enable package scripts" aktiviert?
- Rufen Sie auf der Maschine mit dem App-V-Client und dem VDA im Registrierungseditor (regedit) den Eintrag "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV" auf. Stellen Sie sicher, dass der Schlüssel "AppVServers" den folgenden Wert hat: AppVManagementServer+metadata;PublishingServer (zum Beispiel: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
- Stellen Sie sicher, dass CtxAppVCOMAdmin auf der Maschine mit dem App-V Client und dem VDA Administratorberechtigungen hat. Dies wird normalerweise bei der VDA-Installation erstellt und der lokalen Administratorgruppe auf der VDA-Maschine hinzugefügt. Abhängig von der Active Directory-Richtlinie verliert der Benutzer u. U. die administrative Zuordnung. Führen Sie compmgmt.msc aus und navigieren Sie zu den Benutzern "Lokale Benutzer und Gruppen". Wenn CtxAppVCOMAdmin kein Administrator ist, bearbeiten Sie die Gruppenrichtlinie, damit das Benutzerkonto die administrative Zuordnung behält.
- Prüfen Sie auf der Maschine bzw. dem Masterimage mit dem App-V Client und dem VDA, ob "PowerShell ExecutionPolicy" auf "RemoteSigned" festgelegt ist. Das von Microsoft zur Verfügung gestellte App-V-Clientmodul ist nicht signiert. Mit dieser ExecutionPolicy-Einstellung kann PowerShell unsignierte lokale Skripts und Cmdlets ausführen. Verwenden Sie eine der folgenden Methoden, um ExecutionPolicy festzulegen: (1) Geben Sie als Administrator das Cmdlet **Set-ExecutionPolicy RemoteSigned** ein oder (2) legen Sie über die Gruppenrichtlinieneinstellungen

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

"Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows PowerShell > Skriptausführung aktivieren" fest.

Wenn Sie mit diesen Schritten die Probleme nicht beheben können, aktivieren und prüfen Sie die Protokolle.

Mit App-V zusammenhängende Protokolle sind im Ordner "C:\CtxAppvLogs". Die Anwendungsstartprotokolle sind im Ordner "%LOCALAPPDATA%\Citrix\CtxAppvLogs". LOCALAPPDATA wird in den lokalen Ordner des angemeldeten Benutzers aufgelöst. Prüfen Sie den lokalen Ordner des Benutzers, bei dem der Anwendungsstart fehlschlägt.

Zum Aktivieren der für App-V verwendeten Studio- und VDA-Protokolle müssen Sie Administratorberechtigung haben. Sie benötigen außerdem einen Texteditor (z. B. Editor).

Aktivieren von Studio-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Wechseln Sie zu C:\Programme\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Öffnen Sie CtxAppvCommon.dll.config in einem Texteditor und heben Sie die Auskommentierung der Zeile "" auf.
3. Starten Sie den Brokerdienst neu, um die Protokollierung zu starten.

Aktivieren von VDA-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Wechseln Sie zu C:\Programme\Citrix\Virtual Desktop Agent. Öffnen Sie CtxAppvCommon.dll.config in einem Texteditor und heben Sie die Auskommentierung der Zeile "" auf.
3. Heben Sie die Auskommentierung der folgenden Zeile auf und stellen Sie den Wert auf 1 ein:
4. Starten Sie die Maschine neu, um die Protokollierung zu starten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# AppDisks

Aug 17, 2016

# Übersicht

Die Verwaltung von Anwendungen und der Images, auf denen sie installiert sind, ist nicht unbedingt einfach. Das Citrix Feature AppDisks ist hier eine gute Lösung. AppDisks trennen Anwendungen und Anwendungsgruppen vom Betriebssystem, sodass Sie beides separat verwalten können.

Sie können verschiedene AppDisks mit den Anwendungen für einzelne Benutzergruppen erstellen und dann auf einem Masterimage Ihrer Wahl zusammenstellen. Durch eine solche Gruppierung und Verwaltung von Anwendungen haben Sie mehr Kontrolle über diese und benötigen weniger Masterimages. Dank der so vereinfachten IT-Verwaltung können Sie schneller auf die Anforderungen der Benutzer reagieren. Anwendungen in AppDisks werden über Bereitstellungsgruppen bereitgestellt.

Wenn Ihre Bereitstellung auch Citrix AppDNA enthält, kann es zusammen mit dem AppDisks-Feature verwendet werden. Mit AppDNA können in XenApp und XenDesktop Anwendungen automatisch auf AppDisk-Basis analysiert werden. Mit AppDNA können Sie die Vorzüge des AppDisks-Features optimal nutzen. Die Kompatibilität ohne AppDNA wurde weder getestet noch dokumentiert.

AppDisks unterscheiden sich von anderen Technologien zur Anwendungsbereitstellung in zweierlei Hinsicht: Isolation und Änderungsmanagement.

- Microsoft App-V ermöglicht die Koexistenz nicht kompatibler Anwendungen, indem es diese isoliert. Von AppDisks werden keine Anwendungen isoliert. Stattdessen trennt es die Anwendungen mit den zugehörigen Dateien und Registrierungsschlüsseln vom Betriebssystem. Für Betriebssystem und Benutzer verhalten sich AppDisks so, als wären sie direkt auf einem Masterimage installiert.
- Änderungsmanagement (Masterimageupdate und Testen der Kompatibilität von Updates mit installierten Anwendungen) kann erhebliche Kosten verursachen. AppDNA-Berichte helfen bei der Identifizierung von Problemen und enthalten Lösungsvorschläge. Mit AppDNA können Sie beispielsweise Anwendungen mit gemeinsamen Abhängigkeiten (.NET o. Ä.) finden und auf einem einzelnen gemeinsamen Basisimage installieren. AppDNA ermöglicht auch die Identifizierung von Anwendungen, die beim Betriebssystemstart früh geladen werden, damit Sie sicherstellen können, dass diese ordnungsgemäß funktionieren.

Gut zu wissen:

- Für die Benutzer bleiben die Trennung von Anwendungen vom Betriebssystem und andere Aspekte des AppDisks-Features verborgen. Die Anwendungen verhalten sich so, als wären sie auf dem Image installiert. AppDisks mit komplexen Anwendungen können beim Desktopstart eine geringe Verzögerung verursachen.
- Sie können AppDisks mit gehosteten, freigegebenen Desktops verwenden.
- AppDisks können theoretisch auf Anwendungsbasis masterimage- und betriebssystemübergreifend verwendet werden, dies ist jedoch nicht bei allen Anwendungen möglich. Bei Anwendungen mit einem Skript zur Installation auf einem Desktopbetriebssystem, welches deren Funktion auf einem Serverbetriebssystem nicht zulässt, empfiehlt Citrix die separate Verpackung der Anwendungen für jedes der beiden Betriebssysteme.
- In vielen Fällen funktionieren AppDisks auf unterschiedlichen Betriebssystemen. Sie können beispielsweise eine auf einer Windows 7-VM erstellte AppDisk einer Bereitstellungsgruppe mit Windows 2008 R2-Maschinen hinzufügen, sofern beide


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Betriebssysteme die gleiche Bitanzahl haben (32 oder 64) und die Anwendung unterstützen. Citrix rät allerdings davon ab, eine auf einer neueren Betriebssystemversion (z. B. Windows 10) erstellte AppDisk Bereitstellungsgruppen mit Maschinen hinzuzufügen, auf denen eine ältere Betriebssystemversion (z. B. Windows 7) ausgeführt wird, da es dadurch zu Betriebsstörungen kommen kann.

- Wenn Sie bestimmte Anwendungen auf einer AppDisk nur einer Teilgruppe von Benutzern in einer Bereitstellungsgruppe zugänglich machen möchten, empfiehlt Citrix die Verwendung der Gruppenrichtlinie, um diese Anwendungen vor den anderen Benutzern zu verbergen. Die ausführbare Datei der Anwendung steht weiterhin zur Verfügung, kann für die anderen Benutzer jedoch nicht ausgeführt werden.

# Übersicht über die Bereitstellung

Die folgende Liste bietet eine Übersicht über die Schritte zum Bereitstellen von AppDisks. Einzelheiten finden Sie weiter unten in diesem Artikel.

1. Installieren Sie über die Hypervisor-Verwaltungskonsole einen Virtual Delivery Agent (VDA) auf einer VM.
2. Erstellen Sie über die Hypervisor-Verwaltungskonsole und Studio eine AppDisk.
3. Installieren Sie über die Hypervisor-Verwaltungskonsole Anwendungen auf der AppDisk.
4. Versiegeln Sie die AppDisk über die Hypervisor-Verwaltungskonsole oder über Studio. Durch das Versiegeln können XenApp und XenDesktop die AppDisk-Anwendungen und die zugehörigen Dateien in einer Anwendungsbibliothek (AppLibrary) eintragen.
5. Erstellen oder bearbeiten Sie in Studio eine Bereitstellungsgruppe und wählen Sie die AppDisks dafür aus. Dieser Schritt wird als *Zuweisung von AppDisks* bezeichnet, die verwendete Aktion in Studio heißt dagegen **AppDisks verwalten**. Wenn die VMs in der Bereitstellungsgruppe starten, verteilen XenApp und XenDesktop in Zusammenarbeit mit der AppLibrary, Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) und dem Delivery Controller die ausgewählten AppDisks.

# Anforderungen

Für die Verwendung von AppDisks gelten neben den unter Systemanforderungen aufgeführten Anforderungen einige zusätzlich.

AppDisks werden nur in Bereitstellungen unterstützt, in denen die Version der Delivery Controller und von Studio mindestens der im XenApp- und XenDesktop 7.8-Download entspricht, einschließlich der automatisch installierten Voraussetzungen (.NET 4.5.2 usw.).

AppDisks können auf denselben Windows-Betriebssystemversionen erstellt werden, die auch für VDAs unterstützt werden. Auf den Maschinen in Bereitstellungsgruppen, für die AppDisks verwendet werden sollen, muss mindestens Version 7.8 des VDAs installiert sein.

> Citrix empfiehlt, dass Sie alle Maschinen mit der neuesten VDA-Version installieren oder aktualisieren und dann das Upgrade von Maschinenkatalogen und Bereitstellungsgruppen nach Bedarf durchführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. Dies wird als "Funktionsebene" bezeichnet. Weitere Informationen zur Funktionsebene finden Sie im Artikel Erstellen von Bereitstellungsgruppen.

Zum Bereitstellen von VMs, die zum Erstellen von AppDisks verwendet werden sollen, können Sie Folgendes verwenden:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Die mit Controllerversion 7.8 (Minimum) gelieferte MCS-Version oder die PVS-Version auf der Downloadseite von XenApp und XenDesktop
- Unterstützte XenServer-Releases (s. Artikel zu den Systemanforderungen) oder VMware ab Version 5.1 (AppDisks können nicht mit anderen, für XenApp und XenDesktop unterstützten Hypervisors oder Clouddiensten verwendet werden.)

Das Erstellen von AppDisks wird nicht für Maschinen in MCS-Maschinenkatalogen unterstützt, die temporäre Daten zwischenspeichern.

Remote-PC-Zugriff-Kataloge unterstützen keine AppDisks.

Auf der zum Erstellen einer AppDisk verwendeten VM muss der Windows-Volumeschattenkopie-Dienst aktiviert sein. Der Dienst ist standardmäßig aktiviert.

Mit AppDisks verwendete Bereitstellungsgruppen dürfen Maschinen aus gepoolten zufälligen Maschinenkatalogen mit Serverbetriebssystem- oder Desktopbetriebssystemmaschinen enthalten. Sie können AppDisks nicht mit Maschinen aus anderen Katalogtypen, z. B. solchen mit gepoolten statischen oder dedizierten (zugewiesenen) Maschinen, verwenden.

Auf Maschinen, auf denen Studio installiert ist, muss zusätzlich zu anderen ggf. installierten .NET-Versionen .NET Framework 3.5 installiert sein.

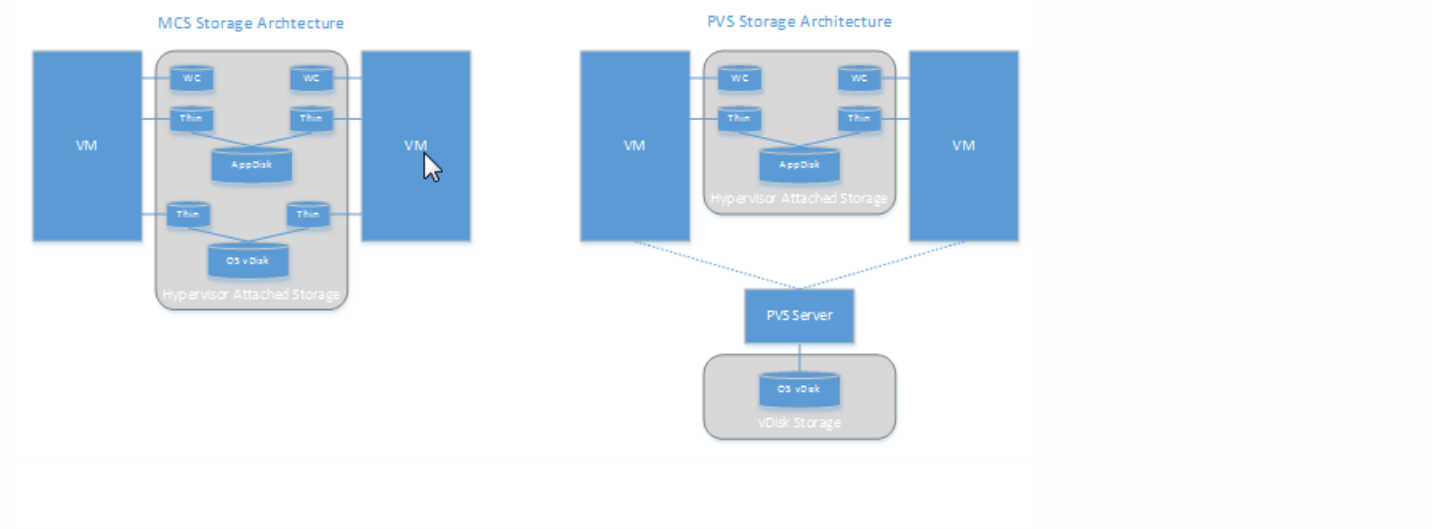
AppDisks können Auswirkungen auf den Speicher haben. Weitere Informationen finden Sie unter Überlegungen zu Speicher und Leistung.

Wenn Sie AppDNA verwenden:

- Lesen Sie die AppDNA-Dokumentation und die AppDisk FAQ.
- Die AppDNA-Software muss auf einem anderen Server als solchen mit Controller installiert werden. Verwenden Sie die mit diesem Release von XenApp und XenDesktop gelieferte AppDNA-Version. Weitere Anforderungen für AppDNA sind in der zugehörigen Dokumentation aufgeführt.
- Stellen Sie sicher, dass auf dem AppDNA-Server eine Firewallausnahme für den Standardport 8199 festgelegt ist.
- Deaktivieren Sie eine bestehende AppDNA-Verbindung beim Erstellen einer AppDisk nicht.
- Beim Erstellen der XenApp- bzw. XenDesktop-Site können Sie die Kompatibilitätsanalyse mit AppDNA auf der Seite **Weitere Features** des Assistenten aktivieren. Sie können diese später über **Konfiguration** > **AppDNA** im Navigationsbereich von Studio aktivieren oder deaktivieren.

Das Trennen von Anwendungen und Betriebssystem durch Verwendung zweier Datenträger und Speichern dieser Datenträger in verschiedenen Bereichen hat Auswirkungen auf die Speicherstrategie. Die folgende Abbildung zeigt die Speicherarchitektur von MCS und PVS. "WC" steht für den Schreibcache und "Thin" für Thin-Datenträger, die zur Speicherung der Unterschiede zwischen den AppDisks und den virtuellen Betriebssystemdatenträgern einer VM verwendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




MCS-Umgebungen

Sie die Größe der AppDisks und Betriebssystem-vDisks gemäß den im Unternehmen geltenden Größenrichtlinien wählen. Werden AppDisks von mehreren Bereitstellungsgruppen verwendet, kann die allgemeine Speicherkapazität reduziert werden.

Da Betriebssystem-vDisks und AppDisks im gleichen Speicherbereich sind, planen Sie den Speicherbedarf sorgfältig, um negative Auswirkungen auf die Kapazität durch die Bereitstellung von AppDisks zu vermeiden. AppDisks erzeugen Mehraufwand. Stellen Sie sicher, dass der Speicher diesen und die Anwendungen abdeckt.

Es gibt keinen Nettoeffekt auf IOPS, da Betriebssystem-vDisks und AppDisks im gleichen Speicherbereich sind. Bei Verwendung von MCS müssen keine Überlegungen in puncto Schreibcache angestellt werden.

PVS-Umgebungen

Sie müssen eine Steigerung von Kapazität und IOPS berücksichtigen, da Anwendungen vom AppDisk-Speicher in den an den Hypervisor angeschlossenen Speicher umsiedeln.

In PVS-Umgebungen verwenden Betriebssystem-vDisks und AppDisks verschiedene Speicherbereiche. Die Speicherkapazität von Betriebssystem-vDisks ist geringer, dafür ist der an den Hypervisor angeschlossene Speicher größer. Sie müssen die Größe Ihrer PVS-Umgebung entsprechend wählen.

AppDisks im am Hypervisor angeschlossenen Speicher erzeugen mehr IOPS, die Betriebssystem-vDisks hingegeben weniger.

Schreibcache: PVS verwendet eine dynamische VHDX-Datei auf einem NTFS-formatierten Laufwerk. Beim Schreiben von Blöcken in den Schreibcache wird die VHDX-Datei dynamisch erweitert. Werden AppDisks einer virtuellen Maschine angefügt, dann werden sie mit den Betriebssystem-vDisks zusammengeführt, um eine einheitliche Ansicht des Dateisystems zu ermöglichen. Beim Zusammenführen werden in der Regel zusätzliche Daten in den Schreibcache geschrieben und die Schreibcachedatei entsprechend größer. Berücksichtigen Sie dies bei der Kapazitätsplanung.

MCS- und PVS-Umgebungen: Verringern Sie die Größe der Betriebssystem-vDisks, um einen Nutzen aus der Verwendung von AppDisks zu ziehen. Wenn Sie dies nicht tun, planen Sie die Verwendung von mehr Speicher ein.

Schalten viele Benutzer in einer Site ihren Computern gleichzeitig ein (beispielsweise zum Beginn des Arbeitstags), kann die Belastung des Hypervisors durch die zahlreichen Startanforderungen sich auf die Leistung auswirken. In PVS-Umgebungen sind die Anwendungen nicht auf der Betriebssystem-vDisk, sodass weniger Anforderungen beim PVS-Server eingehen.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Aufgrund der geringeren Last auf den einzelnen Zielgeräten kann der PVS-Server an mehr Ziele streamen. Eine höhere Ziel-Server-Dichte kann allerdings die Leistung bei einem Boot Storm beeinträchtigen.

# Erstellen von AppDisks

Es gibt zwei Methoden zu Erstellen von AppDisks, Installieren von Anwendungen darauf und Versiegeln der AppDisks. Bei beiden Methoden wird sowohl die Hypervisor-Verwaltungskonsole als auch Studio verwendet. Die Methoden unterscheiden sich darin, wo Sie die meisten der Schritte ausführen.

Bei beiden Methoden gilt Folgendes:

- Setzen Sie für die AppDisk-Erstellung selbst 30 Minuten an.
- Wenn Sie AppDNA verwenden, befolgen Sie die Anweisungen unter "Anforderungen" weiter oben. Deaktivieren Sie eine bestehende AppDNA-Verbindung beim Erstellen einer AppDisk nicht.
- Beim Hinzufügen von Anwendungen zu einer AppDisk stellen Sie sicher, dass Sie die Anwendungen für alle Benutzer installieren. Führen Sie für alle Anwendungen, die die Key Management Server-Aktivierung verwenden, eine Rearm-Operation durch. Weitere Informationen finden Sie in der Anwendungsdokumentation.
- Bei der AppDisk-Erstellung an benutzerspezifischen Orten erstellte Dateien, Ordner und Registrierungseinträge werden nicht beibehalten. Bei einigen Anwendungen wird ein Ersteinsatz-Assistent zum Erstellen von Benutzerdaten während der Installation ausgeführt. Verwenden Sie eine Profilverwaltungslösung, um diese Daten zu speichern und die Anzeige des Assistenten bei jedem AppDisk-Start zu verhindern.
- Bei Verwendung von AppDNA erfolgt direkt nach der Erstellung eine automatische Analyse. Während der Analyse wird als AppDisk-Status in Studio "Analysieren" angezeigt.

AppDisks auf Maschinen aus Maschinenkatalogen, die von Provisioning Services erstellt wurden, erfordern zusätzliche Konfigurationsschritte. Führen Sie in der Provisioning Services Console die folgenden Schritte aus:

1. Erstellen Sie eine neue Version der mit der Gerätesammlung verknüpften vDisk, die die VM enthält.
2. Setzen Sie die VM in den Wartungsmodus.
3. Wählen Sie bei der AppDisk-Erstellung bei jedem VM-Neustart auf dem Startbildschirm die Wartungsversion.
4. Nach dem Versiegeln der AppDisk versetzen Sie die VM wieder in die Produktion und löschen Sie die vDisk-Version, die Sie erstellt haben.

Dieser Vorgang umfasst drei Aufgaben: Erstellen der AppDisk, Erstellen von Anwendungen auf der AppDisk und Versiegeln der AppDisk.

### Erstellen einer AppDisk

1. Wählen Sie im Studio-Navigationsbereich **AppDisks** und im Aktionsbereich **AppDisk erstellen**.
2. Überprüfen Sie die Informationen auf der Seite **Einführung** des Assistenten und klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **AppDisk erstellen** auf das Optionsfeld **Neue AppDisk erstellen**. Wählen Sie eine vordefinierte Datenträgergröße für die AppDisk (klein, mittel, groß) oder geben Sie die Größe in GB ein (Mindestgröße = 3 GB). Die Datenträgergröße muss für die Anwendungen ausreichen, die Sie hinzufügen möchten. Klicken Sie auf **Next**.
4. Wählen Sie auf der Seite **Vorbereitungsmaschine** einen zufälligen gepoolten Katalog zur Verwendung als Masterimage, auf dem die AppDisk erstellt werden soll. Hinweis: Es werden alle Maschinenkataloge der Site nach Typ

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

angezeigt, ausgewählt werden können nur solche, die mindestens eine verfügbare Maschine enthalten. Wenn Sie einen Katalog wählen, der keine zufälligen gepoolten virtuellen Maschinen enthält, schlägt die AppDisk-Erstellung fehl. Nach Auswahl der VM aus einem zufälligen gepoolten Katalog klicken Sie auf **Weiter**.

5. Geben Sie auf der Seite **Zusammenfassung** einen Namen und eine Beschreibung für die AppDisk ein. Überprüfen Sie die auf den vorherigen Seiten des Assistenten angegebenen Informationen. Klicken Sie auf **Fertig stellen**.

Nicht vergessen: Wenn Sie PVS verwenden, folgen Sie den Anweisungen unter "Überlegungen zu PVS".

Nach Schließen des Assistenten wird in Studio für die neue AppDisk "Erstellen" angezeigt. Wenn die AppDisk erstellt ist, wird "Bereit zur Installation von Anwendungen" angezeigt.

### Installieren von Anwendungen auf der AppDisk

Installieren Sie über die Hypervisor-Verwaltungskonsole Anwendungen auf der AppDisk. (**Tipp:** Wenn Sie den Namen der VM vergessen haben, wählen Sie im Studio-Navigationsbereich **AppDisks** und dann im Aktionsbereich **Anwendungen installieren**, um den Namen anzuzeigen.) Informationen zur Installation von Anwendungen finden Sie in der Dokumentation zum Hypervisor. **Nicht vergessen:** Zum Installieren von Anwendungen auf der AppDisk verwenden Sie die Hypervisor-Verwaltungskonsole. Verwenden Sie nicht die Aufgabe "Anwendungen installieren" im Aktionsbereich von Studio.

### Versiegeln der AppDisk

1. Wählen Sie im Studio-Navigationsbereich **AppDisks**.
2. Wählen Sie die erstellte AppDisk und dann im Aktionsbereich **AppDisk versiegeln**.

Nachdem Sie eine AppDisk erstellt, Anwendungen darauf installiert und die AppDisk versiegelt haben, weisen Sie sie einer Bereitstellungsgruppe zu.

Bei diesem Verfahren erstellen Sie die AppDisk über die Hypervisor-Verwaltungskonsole und importieren sie anschließend in Studio.

### Erstellen einer AppDisk, Installieren von Anwendungen und Versiegeln der AppDisk auf dem Hypervisor

1. Erstellen Sie über die Hypervisor-Verwaltungskonsole eine VM und installieren Sie einen VDA.
2. Fahren Sie die Maschine herunter und erstellen Sie einen Snapshot von ihr.
3. Erstellen Sie mit dem Snapshot eine neue Maschine und fügen Sie dieser einen neuen Datenträger hinzu. Der Datenträger (der später zur AppDisk wird) muss groß genug für alle Anwendungen sein, die Sie darauf installieren möchten.
4. Starten Sie die Maschine und wählen Sie **Start > AppDisk vorbereiten**. Ist diese Startmenüverknüpfung auf dem Hypervisor nicht verfügbar, öffnen Sie in C:\Programme\Citrix\personal vDisk\bin eine Eingabeaufforderung und geben Sie **CtxPvD.Exe -s LayerCreationBegin** ein. Die Maschine wird neu gestartet und der Datenträger wird vorbereitet. Ein zweiter Neustart erfolgt, wenn einige Minuten später die Vorbereitung abgeschlossen ist.
5. Installieren Sie die Anwendungen, die Sie den Benutzern zur Verfügung stellen möchten.
6. Doppelklicken Sie auf die Verknüpfung **AppDisk verpacken** auf dem Desktop der Maschine. Die Maschine wird wieder neu gestartet und die Versiegelung beginnt. Wenn das Dialogfeld "In Bearbeitung" geschlossen wird, fahren Sie die VM herunter.

### Importieren der auf dem Hypervisor erstellten AppDisk mit Studio

1. Wählen Sie im Studio-Navigationsbereich **AppDisks** und im Aktionsbereich **AppDisk erstellen**.
2. Überprüfen Sie die Informationen auf der Seite **Einführung** und klicken Sie auf **Weiter**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf der Seite **AppDisk erstellen** auf das Optionsfeld **Vorhandene AppDisk importieren**. Wählen Sie die Ressource (Netzwerk und Speicher), in der die auf dem Hypervisor erstellte AppDisk residiert. Klicken Sie auf **Next**.
4. Navigieren Sie auf der Seite **Vorbereitungsmaschine** zu der Maschine, wählen Sie den Datenträger und klicken Sie dann auf **Weiter**.
5. Geben Sie auf der Seite **Zusammenfassung** einen Namen und eine Beschreibung für die AppDisk ein. Überprüfen Sie die auf den vorherigen Seiten des Assistenten angegebenen Informationen. Klicken Sie auf **Finish**. Die AppDisk wird von Studio importiert.

Wenn Sie die AppDisk in Studio importiert haben, weisen Sie sie einer Bereitstellungsgruppe hinzu.

# Zuweisen einer AppDisk zu einer Bereitstellungsgruppe

Sie können einer Bereitstellungsgruppe beim Erstellen oder später eine oder mehrere AppDisks zuweisen. Dabei verwenden Sie im Prinzip die gleichen AppDisk-Informationen.

Wenn Sie AppDisks einer Bereitstellungsgruppe bei deren Erstellung zuweisen, befolgen Sie die nachfolgenden Anweisungen auf der Seite **AppDisks** des Assistenten. (Informationen zu anderen Seiten des Assistenten finden Sie im Artikel Erstellen von Bereitstellungsgruppen.)

Hinzufügen (oder Entfernen) von AppDisks zu einer vorhandenen Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im Aktionsbereich **AppDisks verwalten**. Informationen zur Seite **AppDisks** finden Sie weiter unten.
3. Wenn Sie die AppDisk-Konfiguration einer Bereitstellungsgruppe ändern, ist ein Neustart der Maschinen in der Gruppe erforderlich. Befolgen Sie auf der Seite **Rolloutstrategie** den Anweisungen unter Erstellen eines Neustartzeitplans.

### Seite "AppDisks"

Die Seite **AppDisks** (im Assistenten zum Erstellen einer Bereitstellungsgruppe bzw. in der AppDisk-Verwaltung) enthält eine Liste der bereits für die Bereitstellungsgruppe bereitgestellten AppDisks und deren Priorität. (Beim Erstellen der Bereitstellungsgruppe ist die Liste leer.) Weitere Informationen finden Sie im Abschnitt AppDisk-Priorität.

1. Klicken Sie auf **Add**. Im Dialogfeld "AppDisks auswählen" werden in der linken Spalte alle AppDisks angezeigt. AppDisks, die der Bereitstellungsgruppe bereits zugewiesen wurden, haben ein aktiviertes Kontrollkästchen und können nicht ausgewählt werden.
2. Wählen Sie mindestens ein Kontrollkästchen einer verfügbaren AppDisk in der linken Spalte aus. In der rechten Spalte werden die Anwendungen auf der jeweiligen AppDisk angezeigt. Auf der Registerkarte **Anwendungen** oberhalb der rechten Spalte werden die Anwendungen in Startmenüformat angezeigt, auf der Registerkarte **Installierte Pakete** ähnelt die Anzeige der Liste "Programme und Features".
3. Nachdem Sie mindestens eine AppDisk gewählt haben, klicken Sie auf **OK**.
4. Klicken Sie auf der Seite "AppDisks" auf **Weiter**.

Wenn einer Bereitstellungsgruppe mehrere AppDisks zugewiesen sind, werden diese auf der Seite **AppDisks** (in den Anzeigen zum Erstellen und Bearbeiten von Bereitstellungsgruppen und zum Verwalten von AppDisks) nach Priorität in


© 1999-2017 Citrix Systems, Inc. All rights reserved.

absteigender Reihenfolge angezeigt. Einträge am Anfang der Liste haben höhere Priorität. Die Priorität gibt an, in welcher Reihenfolge die AppDisks verarbeitet werden.

Sie können die AppDisk-Priorität mit den Pfeilschaltflächen neben der Liste ändern. Ist AppDNA in die AppDisk-Bereitstellung integriert, analysiert es die Anwendungen automatisch und weist die Priorität zu, wenn die AppDisks der Bereitstellungsgruppe zugewiesen werden. Wenn Sie später AppDisks hinzufügen oder aus der Gruppe entfernen,können Sie mit der Option zum automatischen Sortieren eine erneute AppDNA-Analyse der aktuellen AppDisk-Liste zur Bestimmung der Priorität starten. Analyse und Priorisieren (falls erforderlich) können mehrere Minuten dauern.

# Verwalten von AppDisks

Nach dem Erstellen von AppDisks und dem Zuweisen zu Bereitstellungsgruppen können Sie die AppDisk-Eigenschaften über den Knoten "AppDisks" im Navigationsbereich von Studio ändern. Änderungen an den Anwendungen auf einer AppDisk müssen über die Hypervisor-Verwaltungskonsole vorgenommen werden.

**Wichtig:** Sie können den Windows Update-Dienst zum Aktualisieren von Anwendungen (Office-Suite o. Ä.) einer AppDisk verwenden. Verwenden Sie Windows Update jedoch nicht zum Anwenden von Betriebssystemupdates auf AppDisks. Wenden Sie Betriebssystemupdates auf Masterimages und nicht auf AppDisks an, sonst werden die AppDisks nicht richtig initialisiert.

- Wenden Sie nur Patches und andere Updates auf Anwendungen einer AppDisk an, die wirklich für die Anwendungen benötigt werden. Wenden Sie keine für andere Anwendungen vorgesehenen Updates an.
- Bei der Installation von Windows-Updates deaktivieren Sie zunächst alle Einträge und wählen Sie dann nur die Einträge aus, die für die Anwendungen auf der AppDisk erforderlich sind, die Sie aktualisieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Lokaler App-Zugriff und URL-Umleitung

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Anforderungen, Faktoren und Einschränkungen
- Interaktion mit Windows
- Konfigurieren von lokalem App-Zugriff und URL-Umleitung


# Einführung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Computern nötig ist. Lokaler App-Zugriff ermöglicht Folgendes:

- Direkter Zugriff von virtuellen Desktops auf Anwendungen, die lokal auf einem Laptop, PC oder einem anderen Gerät installiert sind
- Bereitstellung einer flexiblen Anwendungsbereitstellungslösung Wenn Benutzer lokale Anwendungen haben, die Sie nicht virtualisieren können oder die IT nicht verwaltet, verhalten sich diese Anwendungen weiterhin so, als ob sie auf einem virtuellen Desktop installiert wären.
- Eliminieren Sie Doppelhoplatenz bei separat vom virtuellen Desktop gehosteten Anwendungen, indem Sie eine Verknüpfung mit der veröffentlichten Anwendung auf das Windows-Gerät des Benutzers platzieren.
- Unter anderem können die folgenden Anwendungen verwendet werden:
  - Videokonferenzsoftware, z. B. GoToMeeting.
  - Spezial- oder Nischenanwendungen, die noch nicht virtualisiert sind.
  - Anwendungen und Peripheriegeräte, die andernfalls große Datenmengen von einem Benutzergerät zum Server und zurück zum Benutzergerät senden würden, wie DVD-Brenner und TV-Tuner.

In XenApp und XenDesktop verwenden gehostete Desktopsitzungen die URL-Umleitung zum Starten von lokalen App-Zugriff-Anwendungen. Durch URL-Umleitung wird die Anwendung unter mehr als einer URL-Adresse bereitgestellt. Durch Auswählen eingebetteter Links in einem Browser in einer Desktopsitzung wird ein lokaler Browser gestartet (basierend auf der URL-Sperrliste des Browsers). Wenn Sie auf eine URL klicken, die nicht auf der Sperrliste steht, wird die URL erneut in der Sitzung geöffnet.

Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen. Für Anwendungssitzungen können Sie nur Host-zu-Client-Inhaltsumleitung verwenden, wobei es sich um eine Art von Server-Dateitypzuordnung handelt. Diese FTA leitet bestimmte Protokolle an den Client um, z. B. HTTP, HTTPS, RTSP oder MMS. Wenn Sie beispielsweise nur eingebettete Links mit HTTP öffnen, werden die Links direkt in der Clientanwendung geöffnet. Für diese Art der Umleitung wird keine URL-Sperrliste oder URL-Positivliste unterstützt.

Wenn der lokale App-Zugriff aktiviert ist, werden URLs, die Benutzern als Links von lokal ausgeführten Anwendungen oder von Benutzern gehosteten Anwendungen bzw. als Verknüpfungen auf dem Desktop angezeigt werden, auf eine der folgenden Arten umgeleitet:

- Umleitung vom Computer des Benutzers zum gehosteten Desktop
- Umleitung vom XenApp- bzw. XenDesktop-Server auf den Computer des Benutzers
- Wiedergabe in der Umgebung, in der sie gestartet werden (keine Umleitung)


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zur Angabe des Pfads für die Inhaltsumleitung von bestimmten Websites konfigurieren Sie die URL-Positivliste und die URL-Sperrliste auf dem Virtual Delivery Agent. Diese Listen enthalten mehrteilige Registrierungsschlüssel, die die Richtlinieneinstellungen für die URL-Umleitung festlegen; weitere Informationen hierzu finden Sie unter "Einstellungen der Richtlinie 'Lokaler App-Zugriff'".

Mit den folgenden Ausnahmen können URLs auf dem VDA wiedergegeben werden:

- Regions-/Gebietsschemainformationen: Websites, die Gebietsschemainformationen benötigen, wie msn.com oder news.google.com (je nach Region wird eine bestimmte Seite geöffnet). Wenn VDA beispielsweise von einem Datenzentrum in Großbritannien bereitgestellt wird und der Client eine Verbindung aus Indien herstellt, würde der Benutzer erwarten, dass die Website in.msn.com erscheint, es wird jedoch uk.msn.com angezeigt.
- Multimedia-Inhalt: Websites mit Rich-Media-Inhalten, die auf dem Clientgerät wiedergegeben werden, ermöglichen eine gewohnte Benutzererfahrung und das Einsparen von Bandbreite während die Funktionalität auch in Netzwerken mit hoher Latenz gewährleistet ist. Die Flash-Umleitung wird durch die Umleitung von Sites mit anderen Medientypen wie Silverlight ergänzt. Somit ist die Umgebung sehr sicher. Die vom Administrator genehmigten URLs werden auf dem Client ausgeführt, während die restlichen URLs an VDA weitergeleitet werden.

Neben der URL-Umleitung können Sie auch FTA-Umleitung (File Type Association = Dateitypzuordnung) verwenden. FTA startet lokale Anwendungen, wenn Dateien in einer Sitzung geöffnet werden sollen. Wenn die lokale Anwendung gestartet wird, muss sie Zugriff auf die Datei haben, um sie zu öffnen. Daher können Sie mit lokalen Anwendungen nur Dateien öffnen, die sich auf Netzwerkfreigaben oder auf Clientlaufwerken (mit Clientlaufwerkzuordnung) befinden. Wenn beispielsweise der PDF-Reader eine lokale Anwendung ist und eine PDF-Datei geöffnet werden soll, wird zum Öffnen der Datei der lokale PDF-Reader verwendet. Da die lokale Anwendung direkt auf die Datei zugreifen kann, erfolgt keine Netzwerkübertragung über ICA zum Öffnen der Datei.

# Anforderungen, Faktoren und Einschränkungen

Lokaler App-Zugriff wird auf den gültigen Betriebssystemen für VDAs für Windows-Serverbetriebssysteme und VDAs für Windows-Desktopbetriebssysteme unterstützt und erfordert mindestens Citrix Receiver für Windows Version 4.1. Die folgenden Browser werden unterstützt:

- Internet Explorer 11. Sie können Internet Explorer 8, 9 oder 10 verwenden, doch die von Microsoft unterstützte und von Citrix empfohlene Version ist Version 11.
- Firefox 3.5 bis 21.0
- Chrome 10

Beachten Sie die folgenden Punkte und Einschränkungen, wenn Sie lokalen App-Zugriff und URL-Umleitung verwenden.

- Lokaler App-Zugriff ist für virtuelle Desktops im Vollbildmodus unter Einbeziehung aller Monitore gedacht:
  - Die Benutzererfahrung kann beeinträchtigt werden, wenn lokaler App-Zugriff auf einem virtuellen Desktop verwendet wird, der im Fenstermodus ausgeführt wird oder der nicht auf allen Monitoren ausgeführt wird.
  - Bei der Verwendung mehrerer Monitore ist der maximierte Monitor der Standarddesktop für alle Anwendungen, die in der Sitzung gestartet werden, selbst wenn nachfolgende Anwendungen normalerweise auf einem anderen Monitor starten würden.
  - Das Feature unterstützt einen VDA; es ist keine Integration mit mehreren gleichzeitigen VDAs möglich.
- Einige Anwendungen können sich unerwartet verhalten und Benutzer beeinträchtigen:
  - Benutzer können die Laufwerkbuchstaben verwechseln, z. B. das lokale C:-Laufwerk mit dem virtuellen C:-Desktoplaufwerk.
  - Auf virtuellen Desktops verfügbare Drucker sind nicht für die lokalen Anwendungen verfügbar.
  - Anwendungen, die erweiterte Berechtigungen erfordern, können nicht als clientgehostete Anwendungen gestartet werden.
  - Keine spezielle Behandlung von Anwendungen mit einer Instanz (z. B. Windows Media Player).
  - Lokale Anwendungen werden mit dem Windows-Design des lokalen Computers angezeigt.
  - Vollbildanwendungen werden nicht unterstützt. Dies schließt Anwendungen ein, die im Vollbildmodus geöffnet werden, z. B. PowerPoint-Bildschirmpräsentationen oder Fotoanzeigen, die den gesamten Desktop ausfüllen.
  - Lokaler App-Zugriff kopiert die Eigenschaften der lokalen Anwendung (z. B. die Verknüpfungen auf dem Clientdesktop und im Startmenü) auf dem VDA. Es werden jedoch keine anderen Eigenschaften, wie Tastenkombinationen und schreibgeschützte Attribute, kopiert.
  - Anwendungen, die die Reihenfolge der überlappenden Fenster anpassen, können unvorhersehbare Ergebnisse verursachen. Beispielsweise könnten einige Fenster ausgeblendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - Verknüpfungen, einschließlich Arbeitsplatz, Papierkorb, Systemsteuerung, Netzlaufwerkverknüpfungen und Ordnerverknüpfungen werden nicht unterstützt.
    - Die folgenden Dateitypen und Dateien werden nicht unterstützt: benutzerdefinierte Dateitypen, Dateien ohne zugeordnete Programme, ZIP-Dateien und ausgeblendete Dateien.
    - Taskleistengruppierung wird nicht für gemischte 32-Bit und 64-Bit clientgehostete Anwendungen und VDA-Anwendungen unterstützt, z. B. die Gruppierung von 32-Bit-Versionen lokaler Anwendungen mit 64-Bit-VDA-Anwendungen.
    - Anwendungen können nicht über COM gestartet werden. Beispiel: Wenn Sie auf ein eingebettetes Office-Dokument in einer Office-Anwendung klicken, wird der Prozessstart nicht erkannt und die Integration der lokalen Anwendung schlägt fehl.
- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen.
- Benutzer haben keine Berechtigung, im lokalen Desktopordner in einer VDA-Sitzung neue Dateien zu erstellen.
- Mehrere Instanzen einer lokal ausgeführten Anwendung verhalten sich entsprechend den Taskleisteneinstellungen für den virtuellen Desktop. Verknüpfungen zu lokal ausgeführten Anwendungen werden jedoch nicht mit ausgeführten Instanzen dieser Anwendungen gruppiert. Sie werden auch nicht mit ausgeführten Instanzen von gehosteten Anwendungen oder mit an gehosteten Anwendungen angehefteten Verknüpfungen gruppiert. Benutzer können nur Fenster von lokal ausgeführten Anwendungen von der Taskleiste aus schließen. Zwar können Benutzer die Fenster von lokalen Anwendungen in der Desktop-Taskleiste und im Startmenü anheften, jedoch starten die Anwendungen bei Verwendung dieser Verknüpfungen möglicherweise nicht konsistent.

# Interaktion mit Windows

Bei der Interaktion zwischen lokaler App-Zugriff und Windows tritt u. a. das folgende Verhalten auf.

- Verknüpfungen in Windows 8 und Windows Server 2012
    - Windows Store-Apps, die auf dem Client installiert sind, werden nicht als Teil der Verknüpfungen von lokalem App-Zugriff aufgelistet.
    - Bild- und Videodateien werden normalerweise standardmäßig mit Windows Store-Apps geöffnet. Lokaler App-Zugriff listet die Windows Store-Apps jedoch auf und öffnet Verknüpfungen mit Desktopanwendungen.
- Local Programs
    - In Windows 7 ist der Ordner im Startmenü verfügbar.
    - In Windows 8 ist der Ordner "Local Programs" nur verfügbar, wenn der Benutzer **Alle Apps** als Kategorie auf der Startseite auswählt. Nicht alle Unterordner werden in Local Programs angezeigt.
- Windows 8-Grafikfunktionen für Anwendungen
    - Desktopanwendungen sind auf den Desktopbereich beschränkt und werden von der Startseite bzw. Anwendungen im Windows 8-Stil vollständig abgedeckt.
    - Mit lokalem App-Zugriff verwendete Anwendungen verhalten sich jedoch bei der Verwendung von mehreren Monitoren nicht wie Desktopanwendungen. Bei der Verwendung mehrerer Monitore werden die Startseite und der Desktop auf unterschiedlichen Monitoren angezeigt.
- Windows 8 und lokaler App-Zugriff mit URL-Umleitung
    - Da bei Windows 8 Internet Explorer keine Add-Ons aktiviert sind, müssen Sie den Desktop-Internet Explorer zum Aktivieren von URL-Umleitung verwenden.
    - In Windows Server 2012 werden Add-Ons von Internet Explorer standardmäßig deaktiviert. Um URL-Umleitung zu implementieren, deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer. Setzen Sie die Internet Explorer-Optionen zurück und starten Sie das Programm neu, um sicherzustellen, dass Add-Ons für Standardbenutzer aktiviert sind.

# Konfigurieren von lokalem App-Zugriff und URL-Umleitung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verwenden von lokalem App-Zugriff und URL-Umleitung für Citrix Receiver:

- Installieren Sie Citrix Receiver auf dem lokalen Clientcomputer. Sie können beide Features während der Installation von Citrix Receiver aktivieren. Alternativ können Sie die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor aktivieren.
- Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Sie können zudem URL-Positivlisten- und Sperrlisten-Richtlinieneinstellungen für die URL-Umleitung konfigurieren. Weitere Informationen finden Sie unter "Einstellungen der Richtlinie 'Lokaler App-Zugriff'".

Aktivieren des lokalen App-Zugriffs und der URL-Umleitung für alle lokalen Anwendungen:

1. Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Mit dieser Einstellung überlässt der VDA dem Client die Entscheidung darüber, ob vom Administrator veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung deaktiviert ist, sind sowohl vom Administrator veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.) Diese Richtlinie gilt für den gesamten Computer als auch für die URL-Umleitungsrichtlinie.
2. Aktivieren Sie den lokalen App-Zugriff und die URL-Umleitung für alle Benutzer eines Computers, wenn Sie Citrix Receiver installieren. Bei dieser Aktion werden die für URL-Umleitung erforderlichen Browser-Add-Ons registriert. Führen Sie an der Eingabeaufforderung den jeweiligen Befehl zum Installieren von Receiver mit der folgenden Option aus:

   **CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1**

   **CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1**

1. Führen Sie **gpedit.msc** aus.
2. Wählen Sie den Knoten **Computerkonfiguration**. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen > Hinzufügen** aus.
3. Fügen Sie die Vorlage icaclient.adm im Citrix Receiver-Konfigurationsordner (normalerweise unter C:\Programme (x86)\Citrix\Online Plugin\Configuration) hinzu. (Nach dem Hinzufügen der Vorlage icaclient.adm zur Computerkonfiguration steht diese auch in der Benutzerkonfiguration zur Verfügung.)
4. Erweitern Sie **Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung**.
5. Wählen Sie **Einstellungen für lokalen App-Zugriff**.
6. Wählen Sie **Aktiviert** und anschließend **URL-Umleitung zulassen**. Registrieren Sie für die URL-Umleitung Browser-Add-Ons über die Befehlszeile wie unten erläutert.

Ermöglichen von Zugriff ausschließlich auf veröffentlichte Anwendungen:

1. Führen Sie auf dem Server, auf dem der Delivery Controller installiert ist, **regedit.exe** aus.
   1. Navigieren Sie zu HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   2. Fügen Sie den REG_DWORD-Eintrag ClientHostedAppsEnabled mit dem Wert 1 hinzu. (Durch den Wert 0 wird der lokale App-Zugriff deaktiviert.)
2. Starten Sie den Delivery Controller-Server neu und starten Sie dann Studio neu.
3. Veröffentlichen Sie lokale App-Zugriff-Anwendungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann die Registerkarte "Anwendungen".
2. Wählen Sie im Aktionsbereich **Anwendung mit lokalem Zugriff erstellen**.
3. Wählen Sie die Desktopbereitstellungsgruppe.
4. Geben Sie den vollständigen Pfad der ausführbaren Datei der Anwendung auf dem lokalen Computer des Benutzers ein.
5. Geben Sie an, ob die Verknüpfung mit der lokalen Anwendung auf dem virtuellen Desktop im Startmenü, auf dem Desktop oder beiden angezeigt wird.
6. Akzeptieren Sie die Standardwerte auf der Seite "Name" und überprüfen Sie die Einstellungen.

4. Aktivieren Sie den lokalen App-Zugriff und die URL-Umleitung für alle Benutzer eines Computers, wenn Sie Citrix Receiver installieren. Bei dieser Aktion werden die für URL-Umleitung erforderlichen Browser-Add-Ons registriert. Führen Sie an der Eingabeaufforderung den Befehl zum Installieren von Citrix Receiver mit der folgenden Option aus:
   **CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1**
   **CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1**
5. Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Mit dieser Einstellung überlässt der VDA dem Client die Entscheidung darüber, ob vom Administrator veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung deaktiviert ist, sind sowohl vom Administrator veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.)

**Hinweis:** Die für URL-Umleitung erforderlichen Browser-Add-Ons werden automatisch registriert, wenn Sie Citrix Receiver über die Befehlszeile mit folgender Option installieren: /ALLOW_CLIENTHOSTEDAPPSURL=1.

Sie können ein Add-On oder alle mit den folgenden Befehlen registrieren und die Registrierung aufheben:

- Registrieren von Add-Ons auf einem Clientgerät: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- Registrierung von Add-Ons auf einem Clientgerät aufheben: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Registrieren von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- Registrierung von Add-Ons auf einem VDA aufheben: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

<*browser*> kann "IE", "FF", "Chrome" oder "All" sein.

Beispiel: Mit dem folgenden Befehl werden Internet Explorer-Add-Ons auf einem Gerät mit Citrix Receiver registriert.

```
C:\Programme\Citrix\ICA Client\redirector.exe/regIE
```

Mit dem folgenden Befehl werden alle Add-Ons auf einem VDA für Windows-Serverbetriebssysteme registriert.

```
C:\Programme (x86)\Citrix\System32\VDARedirector.exe /regAll
```

- Standardmäßig wird die eingegebene URL von Internet Explorer umgeleitet. Wenn die URL nicht in der Sperrliste enthalten ist, aber vom Browser oder der Website an eine andere URL-Adresse umgeleitet wird, wird die endgültige URL nicht umgeleitet, selbst wenn sie auf der Sperrliste steht.

  Zum richtigen Funktionieren der URL-Umleitung müssen Sie bei entsprechender Aufforderung durch den Browser das Add-On aktivieren. Wenn die mit Internetoptionen verbundenen Add-Ons bzw. die angeforderten Add-Ons deaktiviert sind, funktioniert die URL-Umleitung nicht richtig.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Firefox-Add-Ons leiten URLs immer um.

  Wenn ein Add-On installiert wurde, bietet Firefox auf einer neuen Registerkarte die Möglichkeit, die Add-On-Installation zuzulassen oder zu verhindern. Sie müssen das Add-On zulassen, damit das Feature funktioniert.

- Chrome-Add-Ons leiten die endgültige URL stets um, wenn es sich um geleitete und nicht eingegebene URLs handelt.

  Die Erweiterungen wurden extern installiert. Wenn Sie die Erweiterung deaktivieren, funktioniert die URL-Umleitung in Google Chrome nicht. Wenn die URL-Umleitung im Inkognito-Modus erforderlich ist, lassen Sie durch Auswählen dieser Option in den Browsereinstellungen zu, dass die Erweiterung im Inkognito-Modus ausgeführt wird.

1. Führen Sie auf dem gehosteten Desktop **gpedit.msc** aus.
2. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State. Bei 64-Bit-Systemen navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
3. Fügen Sie den REG_DWORD-Eintrag "Terminate" mit einem der folgenden Werte hinzu:
   - 1: Lokale Anwendungen werden weiterhin ausgeführt, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt. Bei der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie in der lokalen Umgebung verfügbar sind.
   - 3: Lokale Anwendungen werden geschlossen, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# XenApp Secure Browser

Jul 08, 2016

Da Anwendungen in das Web portiert werden, müssen Benutzer verschiedene Browser und Browserversionen verwenden, um Kompatibilität mit webbasierten Anwendungen zu erzielen. Wenn es sich bei der Anwendung um eine intern gehostete Anwendung handelt, müssen Organisationen oft komplexe VPN-Lösungen installieren und konfigurieren, um Zugriff für Remotebenutzer zu ermöglichen. Typische VPN-Lösungen erfordern einen clientseitigen Agent, der auf mehreren Betriebssystemen verwaltet werden muss.

Der XenApp Secure Browser ermöglicht Benutzern eine nahtlose webbasierte Anwendungserfahrung, da eine gehostete webbasierte Anwendung in dem vom Benutzer bevorzugten lokalen Browser angezeigt wird. Beispiel: Der bevorzugte Browser eines Benutzers ist Mozilla Firefox, aber die Anwendung ist nur mit Microsoft Internet Explorer kompatibel. XenApp Secure Browser zeigt die mit Internet Explorer kompatible Anwendung als Registerkarte in Firefox an.

# Bereitstellen der XenApp Secure Browser Edition

Citrix empfiehlt, den Lifecycle Management Blueprint für den XenApp Secure Browser zu verwenden, um die Bereitstellung zu vereinfachen. Im Rahmen der Einführung von XenApp 7.9 haben alle vorhandenen XenApp- und XenDesktop-Kunden mit aktiven Software Maintenance- (SWM) oder Subscription Advantage-Abonnements (SA) Zugriff auf die Bereitstellungsedition von Citrix Lifecycle Management.

Der XenApp Secure Browser Blueprint umfasst Scripts zum Automatisieren folgender Aufgaben:

- Installieren von XenApp einschließlich Citrix Lizenzserver und StoreFront
- Erstellen einer XenApp-Bereitstellungssite
- Hinzufügen der bereitgestellten Maschinen zur vorhandenen Domäne

Verwenden des Citrix Lifecycle Management Blueprint

1. Navigieren Sie auf der Homepage von Workspace Cloud zu "Services" und klicken Sie auf "Request Trial for Lifecycle Management". Nachdem Sie die Testversion angefordert haben, erhalten Sie eine E-Mail, wenn die Testversion verfügbar ist. Dies dauert im Allgemeinen 5 bis 10 Minuten.
2. Klicken Sie in der E-Mail auf "Manage", wenn Sie beim Anfordern der Testversion angegeben haben, dass die Seite "Lifecycle Management Overview" angezeigt wird.
3. Laden Sie die ISO-Datei für die Citrix XenApp Secure Browser Edition 7.9 von der Citrix Downloadsite herunter.

Beachten Sie nach dem Download der ISO-Datei für die Secure Browser Edition 7.9 Folgendes:

- Folgen Sie zur Verwendung des XenApp Secure Browser Blueprint den Anleitungen in XenApp Secure Installation with a Citrix Lifecycle Management Blueprint.
- Nach dem Abschluss der Installation optimieren Sie die Umgebung für die Bereitstellung von Web-Apps, indem Sie die in XenApp Secure Browser Deployment Guide beschriebenen Konfigurationsschritte ausführen.

Manuelle Installation von XenApp Secure Browser Version 7.9


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Laden Sie die ISO-Datei für die Citrix XenApp Secure Browser Edition 7.9 von der Citrix Downloadsite herunter.
2. Folgen Sie den Installationsanleitungen für die verschiedenen Komponenten von XenApp.
3. Konfigurieren Sie den Editions- und Lizenzmodus für die Secure Browser Edition nach der Installation, indem Sie die folgenden zusätzlichen Schritte ausführen:

   a. Starten Sie auf dem Delivery Controller eine PowerShell-Sitzung, indem Sie auf der Taskleiste auf das blaue Symbol klicken oder folgende Optionen wählen: Start > Alle Programme > Zubehör >Windows PowerShell > Windows PowerShell.

   **Hinweis**: Auf 64-Bit-Systemen wird damit die 64-Bit-Version gestartet. Es werden die 32-Bit- und 64-Bit-Versionen unterstützt.

   b. Geben Sie "Asnp Citrix*" ein und drücken Sie die Eingabetaste, damit die Citrix spezifischen PowerShell-Module geladen werden.

   **Hinweis**: "Asnp" repräsentiert Add-PSSnapin.

   c. Überprüfen Sie die aktuellen Siteeinstellungen und den Lizenzmodus, indem Sie das Cmdlet Get-ConfigSite ausführen.

   d. Legen Sie den Lizenzmodus auf die XenApp Secure Browser Edition fest, indem Sie den Befehl Set-ConfigSite -ProductCode XDT -ProductEdition BAS ausführen.

   e. Stellen Sie sicher, dass die XenApp Secure Browser Edition und der Lizenzmodus richtig eingerichtet sind, indem Sie das Cmdlet Get-BrokerSite ausführen.

> ## Hinweis
>
> Nach dem Abschluss der Installation optimieren Sie die Umgebung für die Bereitstellung von Web-Apps, indem Sie die unter XenApp Secure Browser Deployment Guide beschriebenen Konfigurationsschritte ausführen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Server-VDI

Aug 17, 2016

Verwenden Sie das Server-VDI-Feature (Virtual Desktop Infrastructure), um einen Desktop von einem Serverbetriebssystem einem einzelnen Benutzer bereitzustellen.

- Enterprise-Administratoren können Serverbetriebssysteme als VDI-Desktops bereitstellen. Dies ist für Benutzer, z. B. Techniker und Designer, nützlich.
- Dienstanbieter können Desktops von der Cloud anbieten. Diese Desktops entsprechen dem Microsoft Services Provider License Agreement (SPLA).

Mit der Citrix Richtlinieneinstellung "Enhanced Desktop Experience" können Sie das Serverbetriebssystem wie ein Windows 7-Betriebssystem aussehen lassen.

Die folgenden Features können nicht mit der Server-VDI verwendet werden:

- Personal vDisks
- Gehostete Anwendungen
- Lokaler App-Zugriff
- Direkte (nicht vermittelte) Desktopverbindungen
- Remote-PC-Zugriff

Server-VDI wird auf den gleichen Serverbetriebssystemen wie der VDA für Windows Serverbetriebssysteme unterstützt.

1. Bereiten Sie den Windows-Server auf die Installation vor: Stellen Sie sicher, dass die Rollendienste "Remotedesktopdienste" nicht installiert sind, und dass Benutzer auf eine Sitzung eingeschränkt sind:
   - Stellen Sie mit dem Windows-Server-Manager sicher, dass die Rollendienste für Remotedesktopdienste nicht installiert sind. Wenn sie installiert sind, entfernen Sie die Dienste.
   - Stellen Sie sicher, dass die Eigenschaft "Nur eine Sitzung pro Benutzer zulassen" aktiviert ist.
     - Unter Windows Server 2008 R2 greifen Sie auf diese Eigenschaft über Verwaltung > Remotedesktopdienste > Remotedesktop-Sitzungshostkonfiguration zu. Im Abschnitt "Einstellungen bearbeiten > Allgemein" muss die Einstellung Nur eine Sitzung pro Benutzer zulassen auf Ja festgelegt sein.
     - Unter Windows Server 2012 bearbeiten Sie die Registrierung und stellen Sie die Terminalservereinstellung ein. Legen Sie für den Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer den Eintrag DWORD fSingleSessionPerUser auf 1 fest.
2. Installieren Sie für Windows Server 2008 R2 Microsoft .NET Framework 3.5 SP1 auf dem Server, bevor Sie den VDA installieren.
3. Installieren Sie einen VDA über die Befehlszeilenschnittstelle mit den Optionen "/quiet" und "/servervdi" auf einem unterstützten Server oder einem Servermasterimage. (In der Standardeinstellung blockiert das Installationsprogramm den VDA für Windows-Desktopbetriebssysteme auf einem Serverbetriebssystem. Mit der Befehlszeile überschreiben Sie dieses Verhalten.)

   **XenDesktopVdaSetup.exe /quiet /servervdi**

   Sie können den oder die Delivery Controller bei der VDA-Installation über die Befehlszeile mit der Option **/controller** festlegen.

   Öffnen Sie mit der Option **/enable_hdx_ports** Ports in der Firewall, wenn die Firewall nicht manuell konfiguriert wird.

   Fügen Sie die Option **/masterimage** hinzu, wenn Sie den VDA auf einem Image installieren, und verwenden Sie MCS zum Erstellen von Server-VMs von diesem Image.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Fügen Sie die Option **/enable_hdx_3d_pro** hinzu, um den VDA im HDX 3D Pro-Modus zu konfigurieren.

Schließen Sie keine Optionen für Features ein, die nicht mit Server-VDI unterstützt werden, u. a. /baseimage oder /xa_server_location.

4. Erstellen Sie einen Maschinenkatalog für Server-VDI.
   1. Klicken Sie auf der Seite Betriebssystem auf **Desktopbetriebssystem**.
   2. Geben Sie auf der Seite Zusammenfassung einen Maschinenkatalognamen und eine Beschreibung für Administratoren an, die ausdrücklich Server-VDI angeben. Dies ist die einzige Angabe in Studio, dass der Katalog Server-VDI unterstützt.

   Wenn Sie eine Suche in Studio durchführen, wird der erstellte Server-VDI-Katalog auf der Registerkarte "Desktopbetriebssystemmaschinen" angezeigt, obwohl der VDA auf einem Server installiert wurde.

5. Erstellen Sie eine Bereitstellungsgruppe und weisen Sie den Server-VDI-Katalog zu, den Sie im letzten Schritt erstellt haben.

Wenn Sie während der Installation des VDA keinen Delivery Controller festgelegt haben, geben sie ihn später über eine Citrix Richtlinieneinstellung, Active Directory oder durch Bearbeiten der Registrierungswerte des VDA-Computers an.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Personal vDisk

Jul 08, 2016

Das Personal vDisk-Feature bietet die Einzelimageverwaltung für gepoolte und gestreamte Desktops, während Benutzer Anwendungen installieren und ihre Desktopeinstellungen anpassen können. Im Gegensatz zu traditionellen Virtual Desktop Infrastructure (VDI)-Bereitstellungen mit gepoolten Desktops, bei denen Benutzer Anpassungen und eigene Anwendungen verlieren, wenn der Administrator das Masterimage ändert, werden in Bereitstellungen mit persönlichen vDisks diese Änderungen beibehalten. Dies bedeutet, dass Administratoren die Masterimages auf einfache Weise zentral verwalten können, während Benutzer gleichzeitig von einer individuell angepassten Desktoperfahrung profitieren.

Persönliche vDisks erreichen diese Trennung, indem Sie alle auf der VM des Benutzers vorgenommenen Änderungen an einen separaten Datenträger, die persönliche vDisk, weiterleiten, die mit der VM des Benutzers verknüpft ist. Der Inhalt der persönlichen vDisk wird zur Laufzeit mit dem Inhalt des Masterimages zusammengeführt, um eine einheitliche Erfahrung zu gewährleisten. Auf diese Weise können Benutzer immer noch auf die Anwendungen zugreifen, die der Administrator auf dem Masterimage zur Verfügung gestellt hat.

Persönliche vDisks bestehen aus zwei Teilen, die unterschiedliche Laufwerksbuchstaben verwenden und ungefähr gleich groß sind:

- Benutzerprofil: Dieser Teil enthält Benutzerdaten, Dokumente und das Benutzerprofil. Standardmäßig wird hierfür Laufwerk P: verwendet, Sie können aber einen anderen Laufwerksbuchstaben wählen, wenn Sie einen Maschinenkatalog mit Maschinen erstellen, die persönliche vDisks verwenden. Das verwendete Laufwerk hängt auch von der Einstellung für EnableUserProfileRedirection ab.
- Virtual Hard Disk-Datei (.vhd): Dieser Teil enthält alle anderen Objekte, z. B. Anwendungen, die unter C:\Programme installiert sind. Dieser Teil wird nicht in Windows Explorer angezeigt und benötigt seit Version 5.6.7 keinen Laufwerksbuchstaben.

Mit persönlichen vDisks können Anwendungen auf Abteilungsebene bereitgestellt werden und sie unterstützen auch Anwendungen, die von Benutzern heruntergeladen und installiert wurden, einschließlich solcher, für die Treiber (außer Phase-1-Treiber), Datenbanken und Maschinenverwaltungssoftware erforderlich ist. Wenn die Änderung eines Benutzers mit der Änderung eines Administrators kollidiert, können diese Änderungen mit einer persönlichen vDisk leicht und automatisch abgestimmt werden.

Außerdem können lokal verwaltete Anwendungen (z. B. solche, die von lokalen IT-Abteilungen bereitgestellt werden) auch in der Umgebung des Benutzers bereitgestellt werden. Der Benutzer bemerkt keine Unterschiede bei der Verwendung; mit persönlichen vDisks wird sichergestellt, dass alle Änderungen und alle installierten Anwendungen auf der vDisk gespeichert werden. In Fällen, bei denen eine Anwendung auf einer persönlichen vDisk genau mit einer Anwendung auf einem Masterimage übereinstimmt, wird die Version auf der persönlichen vDisk aus Platzspargründen verworfen, ohne dass der Benutzer den Zugriff auf die Anwendung verliert.

Persönliche vDisks werden physisch auf dem Hypervisor gespeichert, sie müssen sich aber nicht am gleichen Speicherort befinden wie andere auf dem virtuellen Desktop bereitgestellte Datenträger. Dadurch können sich die Kosten für persönlichen vDisk-Speicher verringern.

Wenn Sie während der Site-Erstellung eine Verbindung erstellen, legen Sie Speicherorte für die Datenträger fest, die von den virtuellen Maschinen verwendet werden. Sie können die persönlichen vDisks von den Datenträgern für das Betriebssystem trennen. Jede VM muss Zugriff auf den Speicherort der beiden Datenträger haben. Wenn Sie für beide lokalen Speicher verwenden, muss der Hypervisor in der Lage sein, auf beide zuzugreifen. Um dies zu gewährleisten, bietet Studio nur


© 1999-2017 Citrix Systems, Inc. All rights reserved.

kompatible Speicherorte an. Später können Sie auch über "Konfiguration > Hosting" in Studio persönliche vDisks und Speicher dafür vorhandenen Hosts (aber nicht Maschinenkatalogen) hinzufügen.

Erstellen Sie regelmäßig ein Backup der persönlichen vDisks mit der bevorzugten Methode. vDisks sind standardmäßige Volumes in der Speicherebene eines Hypervisors. Sie können genauso wie andere Volumes gesichert werden.

## Neue Features in Personal vDisk 7.6.1

Dieses Release enthält folgende Verbesserungen:

- Diese Version von Personal vDisk enthält Leistungsverbesserungen, durch die die zum Anwenden eines Imageupdates auf einen Personal vDisk-Katalog benötigte Zeit verkürzt wird.

Die folgenden Probleme wurden in diesem Release behoben:

- Bei dem Versuch, eine Basis-VM mit einem direkten Upgrade von Microsoft Office 2010 auf Microsoft Office 2013 zu aktualisieren, wurde dem Benutzer ein Konfigurationsfenster gefolgt von der folgenden Fehlermeldung angezeigt: "Error 25004. The product key you entered cannot be used on this machine." Zuvor wurde in diesem Fall empfohlen, Office 2010 auf der Basis-VM zu deinstallieren und danach Office 2013 zu installieren. Jetzt ist es nicht mehr nötig, Office 2010 beim Durchführen eines direkten Upgrades auf der Basis-VM zu deinstallieren (#391225).
- Wenn während eines Imageupdates eine höhere Version von Microsoft .Net auf der persönlichen vDisk des Benutzers gefunden wurde, wurde diese vom Basisimage mit einer niedrigeren Version überschrieben. Dies führte für Benutzer zu Problemen beim Ausführen bestimmter, auf ihrer persönlichen vDisk installierter Anwendungen, die eine höhere Version, z. B. Visual Studio, benötigten (#439009).
- Ein mit Provisioning Services bereitgestellter Datenträger, auf dem Personal vDisk installiert und aktiviert ist, kann nicht zum Erstellen eines nicht-Personal vDisk-Maschinenkatalogs verwendet werden. Diese Einschränkung wurde entfernt (#485189).

## Info zu Personal vDisk 7.6

Neue Features in Version 7.6:

- Verbesserte Fehlerbehandlung und Berichterstellung für Personal vDisk. Wenn Sie in Studio PvD-aktivierte Maschinen in einem Katalog anzeigen, können Sie auf der Registerkarte "PvD" den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Außerdem wurden die Zustandsanzeigen verbessert.
- Ein Überwachungstool für PvD-Imageupdates ist für frühere Versionen auf dem ISO-Medium verfügbar (ISO\Support\Tools\Scripts\PvdTool). Überwachungsfunktionen wurden auch in früheren Releases unterstützt, jedoch sind die Berichterstellungsfunktionen nicht so robust wie im aktuellen Release.
- Im Provisioning Services-Testmodus können Sie Maschinen mit einem aktualisierten Image in einem Testkatalog starten. Nachdem Sie die Stabilität überprüft haben, können Sie die Testversion der persönlichen vDisk auf "Production" hochstufen.
- Mit einer neuen Funktion können Sie das Delta (die Differenz) zwischen zwei Beständen während einer Bestandsaktualisierung berechnen statt sie für jeden PvD-Desktop einzeln berechnen zu müssen. Es sind neue Befehle zum Exportieren und Importieren eines vorherigen Bestands für MCS-Kataloge verfügbar. (Provisioning Services-Master-vDisks haben bereits den vorherigen Bestand.)

Bekannte Probleme aus Version 7.1.3, die in Version 7.6 behoben wurden:

- Unterbrechen des Upgrades einer Personal vDisk-Installation kann dazu führen, dass eine vorhandene Personal vDisk-Installation beschädigt wird. [#424878]
- Ein virtueller Desktop reagiert möglicherweise nicht mehr, wenn die persönliche vDisk über einen langen Zeitraum ausgeführt wird und es zu einem Speicherverlust im nicht-ausgelagerten Speicher kommt. [#473170]

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Neue bekannten Probleme in Version 7.6:

- Das Vorhandensein von Antivirenprodukten kann sich darauf auswirken, wie lange das Durchführen einer Bestandsaktualisierung oder eines Updates dauert. Die Leistung kann verbessert werden, wenn Sie CtxPvD.exe und CtxPvDSvc.exe der PROCESS-Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal vdisk\bin. [#326735]
- Feste Links zwischen Dateien, die vom Masterimage geerbt wurden, bleiben in persönlichen vDisk-Katalogen nicht erhalten. [#368678]
- Nach dem Upgrade von Office 2010 auf 2013 auf dem Personal vDisk-Masterimage kann Office nicht auf virtuellen Maschinen gestartet werden, da der KMS-Lizenzierungsproduktschlüssel von Office beim Upgrade entfernt wurde. Als Workaround können Sie Office 2010 deinstallieren und Office 2013 auf dem Masterimage neu installieren. [#391225]
- Personal vDisk-Kataloge unterstützen keine VMware Paravirtual SCSI (PVSCSI)-Controller. Verwenden Sie den Standardcontroller, um dieses Problem zu vermeiden. [#394039]
- Für virtuelle Desktops, die mit Personal vDisk Version 5.6.0 erstellt wurden und auf 7 aktualisiert werden, finden Benutzer, die sich an der Master-VM anmelden, nicht alle Dateien in der gepoolten VM. Dieses Problem tritt auf, da ein neues Benutzerprofil erstellt wird, wenn sich Benutzer an der gepoolten VM anmelden. Für dieses Problem gibt es keinen Workaround. [#392459]
- Personal vDisks, die unter Windows 7 ausgeführt werden, können das Feature "Sichern und Wiederherstellen" nicht verwenden, wenn der Windows-Systemschutz aktiviert ist. Wenn der Systemschutz deaktiviert ist, wird ein Backup des Benutzerprofils aber nicht der Datei userdata.v2.vhd erstellt. Citrix empfiehlt, den Systemschutz zu deaktivieren und ein Backup des Benutzerprofils mit dem Feature "Sichern und Wiederherstellen" zu erstellen. [#360582]
- Beim Erstellen einer VHD-Datei auf der Basis-VM mit dem Datenträgerverwaltungstool können Sie die virtuelle Festplatte (VHD) möglicherweise nicht bereitstellen. Um dieses Problem zu umgehen, kopieren Sie die VHD auf das PvD-Volume. [#355576]
- Office 2010-Verknüpfungen bleiben auf virtuellen Desktops erhalten, nachdem diese Software entfernt wurde. Um dieses Problem zu umgehen, löschen Sie die Verknüpfungen. [#402889]
- Wenn Sie Microsoft Hyper-V verwenden, können Sie mit Maschinen mit persönlichen vDisks keinen Katalog erstellen, wenn die Maschinen lokal gespeichert sind und die vDisks auf freigegebenen Clustervolumes (CSVs) gespeichert sind. Die Katalogerstellung schlägt fehl und ein Fehler wird angezeigt. Um dieses Problem zu umgehen, verwenden Sie einen anderen Speicherort für die vDisks. [#423969]
- Wenn Sie sich das erste Mal bei einem virtuellen Desktop anmelden, der von einem Provisioning Services-Katalog erstellt wurde, werden Sie aufgefordert, den Desktop neu zu starten, wenn die persönliche vDisk zurückgesetzt wurde (mit dem Befehl "ctxpvd.exe -s reset"). Um dieses Problem zu lösen, starten Sie den Desktop neu, wenn Sie dazu aufgefordert werden. Es handelt sich hier um eine einmalige Zurücksetzung, die bei erneuter Anmeldung nicht erforderlich ist. [#340186]
- Wenn Sie .NET 4.5 auf einer persönlichen vDisk installieren und .NET 4.0 bei einem späteren Update des Images installiert oder bearbeitet wird, schlagen Anwendungen, die von .NET 4.5 abhängig sind, fehl. Um dieses Problem zu umgehen, stellen Sie .NET 4.5 vom Basisimage aus als Imageupdate bereit.
- Weitere Informationen finden Sie unter
  *— Bekannte Probleme*
  in der Dokumentation zu XenApp und XenDesktop 7.6.

## Info zu Personal vDisk 7.1.3

Bekannte Probleme aus Version 7.1.1, die in Version 7.1.3 behoben wurden:

- Direkte Upgrades von Personal vDisk 5.6.0 auf Personal vDisk 7.x können zu Fehlern bei Personal vDisk führen. [#432992]
- Benutzer können möglicherweise nur zeitweilig Verbindungen zu virtuellen Desktops mit persönlichen vDisks herstellen. [#437203]


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Wenn das Update eines Personal vDisk-Images während der Aktualisierung von Personal vDisk 5.6.5 oder höher auf Personal vDisk 7.0 oder höher unterbrochen wird, können spätere Updates fehlschlagen. [#436145]

### Info zu Personal vDisk 7.1.1

Bekannte Probleme aus Version 7.1, die in Version 7.1.1 behoben wurden:

- Nach der Aktualisierung auf Symantec Endpoint Protection 12.1.3 über ein Imageupdate meldet symhelp.exe beschädigte Antivirus-Definitionen. [#423429]
- Personal vDisk kann den Neustart gepoolter Desktops verursachen, wenn der Dienststeuerungs-Manager (services.exe) abstürzt. [#0365351]

Neue bekannten Probleme in Version 7.1.1: Keine

### Info zu Personal vDisk 7.1

Neue Features in Version 7.1:

- Sie können Personal vDisk nun auch auf Desktops unter Windows 8.1 verwenden und die Ereignisprotokollierung wurde verbessert.
- Copy-on-Write (CoW) wird nicht mehr unterstützt. Beim Upgrade von Personal vDisk Version 7.0 auf 7.1 gehen alle von CoW verwalteten Datenänderungen verloren. CoW war ein Feature, das in XenDesktop 7 bewertet wurde und standardmäßig deaktiviert war. Wenn Sie es nicht aktiviert haben, sind Sie nicht betroffenen.

Bekannte Probleme aus Version 7.0.1, die in Version 7.1 behoben wurden:

- Wenn der Wert des Personal vDisk-Registrierungsschlüssels EnableProfileRedirection auf 1 oder ON eingestellt ist, und Sie den Wert beim Aktualisieren des Images in 0 oder OFF ändern, wird der ganze Personal vDisk-Speicherplatz u. U. den vom Benutzer installierten Anwendungen zugeordnet, sodass kein Platz für Benutzerprofile vorhanden ist, die auf der vDisk bleiben. Wenn die Profilumleitung für einen Katalog deaktiviert ist und Sie die Profilumleitung während eines Imageupdates aktivieren, können sich Benutzer u. U. nicht bei ihren virtuellen Desktops anmelden. [#381921]
- Der Desktopdienst protokolliert nicht den richtigen Fehler in der Ereignisanzeige, wenn das Update des Personal vDisk-Bestands fehlschlägt. [#383331]
- Beim Upgrade auf Personal vDisk 7.x bleiben geänderte Regeln nicht erhalten. Dieses Problem wurde für das Upgrade von Version 7.0 auf Version 7.1 behoben. Beim Upgrade von Version 5.6.5 auf Version 7.1 müssen Sie die Regeldatei zuerst speichern und die Regeln nach dem Upgrade erneut anwenden. [#388664]
- Personal vDisks, die unter Windows 8 ausgeführt werden, können keine Anwendungen vom Windows Store installieren. Eine Fehlermeldung gibt an, dass der Kauf nicht abgeschlossen werden konnte. Wenn Sie den Windows Update-Dienst aktivieren, wird das Problem nun behoben. Von Benutzern installierte Anwendungen müssen jedoch nach dem Neustart des Systems neu installiert werden. [#361513]
- Einige symbolische Verknüpfungen fehlen auf gepoolten Windows 7-Desktops mit persönlichen vDisks. Daher werden Symbole, die von Anwendungen unter C:\Benutzer\Alle Benutzer gespeichert werden, nicht im Startmenü angezeigt. [#418710]
- Der Start einer persönlichen vDisk schlägt fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. [#369846]
- Der Start einer persönlichen vDisk schlägt fehl und der Statuscode 0x20 sowie Fehlercode 0x20000028 werden angezeigt. [#393627]
- Symantec Endpoint Protection 12.1.3 zeigt die Fehlermeldung "Proactive Threat Protection is malfunctioning" an und der Liveupdatestatus dieser Komponente ist nicht verfügbar. [#390204]

Neue bekannte Probleme in Version 7.1: Weitere Informationen finden Sie unter

*— Bekannte Probleme*


© 1999-2017 Citrix Systems, Inc. All rights reserved.

in der Dokumentation zu XenDesktop 7.1.

## Info über Personal vDisk 7.0.1

Neu in Version 7.0.1: Personal vDisk ist jetzt robuster bei Änderungen der Umgebung. Virtuelle Desktops mit persönlichen vDisks werden jetzt beim Delivery Controller registriert, selbst wenn das Imageupdate fehlschlägt, und das Herunterfahren von unsicheren Systemen setzt die vDisks in einen permanent deaktivierten Zustand. Darüber hinaus können Sie nun während einer Bereitstellung Dateien und Ordner mithilfe von Regeldateien von vDisks ausschließen.

Bekannte Probleme aus Version 5.6.13, die in Version 7.0.1 behoben wurden:

- Änderungen an der Mitgliedschaft einer Gruppe, die von einem Benutzer an einem gepoolten virtuellen Desktop vorgenommen wurden, gehen u. U. nach einem Imageupdate verloren. [#286227]
- Imageupdates schlagen u. U. mit einer Fehlermeldung, dass der Speicherplatz auf dem Datenträger niedrig ist, fehl, selbst wenn die persönliche vDisk genug Speicherplatz hat. [#325125]
- Die Installation einiger Anwendungen schlägt auf virtuellen Desktops mit einer persönlichen vDisk fehl, und eine Meldung weist auf einen erforderlichen Neustart hin. Grund ist eine ausstehende Umbenennung. [#351520]
- Symbolische Links, die im Masterimage erstellt wurden, funktionieren nicht auf virtuellen Desktops mit persönlichen vDisks. [#352585]
- In Umgebungen mit der Citrix Profilverwaltung und Personal vDisk funktionieren Anwendungen, die Benutzerprofile auf einem Systemvolume überprüfen u. U. nicht richtig, wenn die Profilumleitung aktiviert ist. [#353661]
- Die Bestandsaktualisierung schlägt auf Masterimages fehl, wenn der Bestand größer als 2 GB ist. [#359768]
- Imageupdates schlagen mit einem Fehlercode 112 fehl und persönliche vDisks sind beschädigt, selbst wenn die vDisks ausreichend Speicherplatz für das Update haben. [#363003]
- Das Skript für das Ändern der Größe schlägt für Kataloge fehl, die mehr als 250 Desktops haben. [#363365]
- Benutzerseitige Änderungen einer Umgebungsvariablen gehen bei einer Aktualisierung des Images verloren. [#372295]
- Lokale Benutzer, die auf einem virtuellen Desktop mit einer persönlichen vDisk erstellt wurden, gehen bei einer Aktualisierung des Images verloren. [#377964]
- Der Start einer persönlichen vDisk schlägt u. U. fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. Erhöhen Sie die USN-Journalgröße im Masterimage auf mindestens 32 MB und aktualisieren Sie das Image, um dieses Problem zu vermeiden. [#369846]
- Ein Problem wurde mit Personal vDisk festgestellt, das ein richtiges Funktionieren der Registrierungsstrukturaktionen des AppSense-Umgebungs-Managers verhindert, wenn AppSense im Ersetzenmodus verwendet wird. Citrix und AppSense arbeiten an der Behebung des Problems, das mit dem Verhalten der RegRestoreKey-API zusammenhängt, wenn Personal vDisk installiert ist. [#0353936]

## Release-unabhängige bekannte Probleme

- Wenn eine Anwendung auf einer persönlichen vDisk (PvD) mit einer auf dem Masterimage installierten anderen Anwendung derselben Version verbunden ist, funktioniert die Anwendung auf der PvD nach einem Imageupdate möglicherweise nicht mehr. Dieses Problem tritt auf, wenn die Anwendung vom Masterimage deinstalliert oder auf eine neuere Version aktualisiert wird, da durch diese Aktion die Dateien entfernt werden, die die Anwendung auf der PvD vom Masterimage benötigt. Um dies zu verhindern, lassen Sie die Anwendung mit den Dateien, die von der Anwendung auf der PvD benötigt werden, auf dem Masterimage.
  Beispiel: Das Masterimage enthält Office 2007 und ein Benutzer installiert Visio 2007 auf der PvD. Die Office-Anwendungen und Visio funktionieren einwandfrei. Später ersetzt der Administrator Office 2007 durch Office 2010 auf dem Masterimage und aktualisiert anschließend alle betroffenen Maschinen mit dem aktualisierten Image. Visio 2007 funktioniert nicht mehr. Um dies zu verhindern, lassen Sie Office 2007 auf dem Masterimage. [#320915]

- Wenn Personal vDisk verwendet wird, verwenden Sie bei der Bereitstellung von McAfee Virus Scan Enterprise (VSE) die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Version 8.8 Patch 4 oder höher auf einem Masterimage. [#303472]

- Wenn eine Verknüpfung für eine Datei auf dem Masterimage nicht mehr funktioniert, weil das Verknüpfungsziel in PvD umbenannt wurde, erstellen Sie die Verknüpfung neu. [#367602]
- Verwenden Sie keine absoluten bzw. festen Links auf einem Masterimage. [#368678]
- Das mit Windows 7 verfügbare Feature "Sichern und Wiederherstellen" wird auf der persönlichen vDisk nicht unterstützt. [#360582]
- Nach der Anwendung eines aktualisierten Masterimages ist kein Zugriff auf die Konsole für lokale Benutzer und Gruppen möglich oder sie zeigt inkonsistente Daten an. Um das Problem zu lösen, setzen Sie die Benutzerkonten auf der VM zurück. Dazu muss die Sicherheitsstruktur zurückgesetzt werden. Dieses Problem wurde im Release 7.1.2 behoben und löst auch das Problem für VMs in späteren Releases, aber nicht für VMs, die mit einer früheren Version erstellt und dann aktualisiert wurden. [#488044]
- Bei der Verwendung einer gepoolten VM in einer ESX Hypervisor-Umgebung wird Benutzern eine Neustartaufforderung angezeigt, wenn der ausgewählte SCSI-Controllertyp ein "VMware Paravirtual" ist. Um dieses Problem zu umgehen, verwenden Sie den Controllertyp "LSI SCSI". [#394039]
- Nach dem Zurücksetzen von PvD auf einem mit Provisioning Services erstellten Desktop wird Benutzern nach der Anmeldung an der VM u. U. eine Neustartaufforderung angezeigt. Um dieses Problem zu umgehen, starten Sie den Desktop neu. [#340186]
- Benutzer von Windows 8.1-Desktops können sich u. U. nicht an ihren PvDs anmelden. Einem Administrator wird möglicherweise die Meldung "PvD was disabled due to unsafe shutdown" angezeigt und das PvDActivation-Protokoll enthält u. U. die Meldung "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]". Dieses Problem tritt auf, wenn die VM nicht sicher heruntergefahren wird. Sie umgehen das Problem, indem Sie die persönliche vDisk zurücksetzen. [#474071]


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installation und Upgrade

Jul 08, 2016

Personal vDisk 7.x wird seit XenDesktop 5.6 bis zur aktuellen Version unterstützt. Für jede XenDesktop-Version werden in der Dokumentation unter "Systemanforderungen" die unterstützten Betriebssysteme für Virtual Delivery Agents (VDAs) sowie die unterstützten Versionen von Hosts (Virtualisierungsressourcen) und Provisioning Services aufgelistet. Weitere Informationen zu Provisioning Services-Aufgaben finden Sie in der Dokumentation zu Provisioning Services.

## Installieren und Aktivieren von PvD

PvD wird automatisch installiert, wenn Sie einen VDA für Desktopbetriebssysteme auf einer Maschine installieren oder aktualisieren. Wenn Sie die PvD-Software nach der Installation des VDAs aktualisieren, verwenden Sie die PvD-MSI, die auf dem XenApp- oder XenDesktop-Installationsmedium verfügbar ist.

Aktivieren von PvD:

- PvD wird automatisch aktiviert, wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Maschinenkatalog erstellen, dessen Desktopbetriebssystemmaschinen eine persönliche vDisk verwenden.
- Wenn Sie Provisioning Services (PVS) verwenden, wird PvD automatisch aktiviert, wenn Sie während der Erstellung des Masterimages den Bestand aufnehmen oder wenn bei einem automatischen Update der Bestand aktualisiert wird.

Während der VDA-Installation haben Sie die Möglichkeit, PvD zu aktivieren, indem Sie das Kontrollkästchen "Personal vDisk" auf der grafischen Benutzeroberfläche auswählen oder über die Befehlszeilenschnittstelle die Option "/baseimage" angeben. Auch wenn Sie diese Aktion bei der Installation des VDAs (Standard) nicht ausführen, können Sie mit dem gleichen Image PvD-Desktops und Desktops ohne PvD erstellen, da PvD während der Katalogerstellung aktiviert wird.

## Hinzufügen von persönlichen vDisks

Sie fügen Hosts persönliche vDisks hinzu, wenn Sie eine Site konfigurieren. Sie können denselben Speicher auf dem Host für VMs und persönliche vDisks verwenden oder Sie können einen anderen Speicher für persönliche vDisks auswählen.

Später können Sie auch persönliche vDisks und ihren Speicher vorhandenen Hosts (Verbindungen), jedoch nicht Maschinenkatalogen, hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie im Aktionsbereich Persönlichen vDisk-Speicher hinzufügen und geben Sie einen Speicherort an.

## Aktualisieren von PvD

Die einfachste Methode, Personal vDisk von einer früheren 7.x-Version zu aktualisieren, ist das Aktualisieren der VDAs für Desktopbetriebssysteme mit der aktuellen XenDesktop-Version. Nehmen Sie anschließend den PvD-Bestand auf.

Sie können auch nur PvD mit der hier verfügbaren PvD-MSI aktualisieren.

## Deinstallieren von PvD

Sie können die PvD-Software mit einer der folgenden beiden Methoden deinstallieren:

- Deinstallieren Sie den VDA. Dabei wird die PvD-Software ebenfalls entfernt.
- Wenn Sie PvD mit der PvD-MSI aktualisiert haben, können Sie es über die Liste der Programme deinstallieren.

Wenn Sie PvD deinstallieren und dieselbe oder eine neuere Version neu installieren, erstellen Sie eine Sicherungskopie des Registrierungsschlüssels HKLM\Software\Citrix\personal vDisk\config, der Konfigurationseinstellungen für die Umgebung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

enthält, die sich geändert haben können. Nach der Installation von PvD können Sie die Registrierungswerte, die sich geändert haben, durch einen Vergleich mit der Sicherungskopie zurücksetzen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren und Verwalten

Jul 08, 2016

In diesem Abschnitt werden Themen erläutert, die beim Konfigurieren und Verwalten einer Personal vDisk (PvD)-Umgebung zu berücksichtigen sind. Darüber hinaus werden Best Practices und Aufgabenbeschreibungen behandelt.

Beachten Sie Folgendes beim Arbeiten in der Windows-Registrierung:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

## Überlegungen zur Größe einer persönlichen vDisk

Die folgenden Faktoren beeinflussen die Größe des PvD-Haupvolumes:

- **Größe der Anwendungen, die Benutzer auf ihren PvDs installieren**
  Bei Neustarts bestimmt PvD den im Anwendungsbereich verbleibenden freien Speicherplatz (UserData.v2.vhd). Wenn dieser Wert unter 10 % fällt, wird der Anwendungsbereich erweitert, indem ungenutzter Speicherplatz des Profilbereichs (standardmäßig der freie Speicherplatz auf dem Laufwerk P:) genutzt wird. Der zum Anwendungsbereich hinzugefügte Speicherplatz beträgt ungefähr 50 % des zusammengefassten freien Speicherplatzes von Anwendungs- und Profilbereich.

  Beispiel: Wenn der Anwendungsbereich auf einer 10 GB PvD, der standardmäßig eine Größe von 5 GB hat, den Wert 4,7 GB erreicht und der Profilbereich über 3 GB freien Speicherplatz verfügt, wird der zusätzliche Speicherplatz wie folgt berechnet:

  erweiterter Speicherplatz = (5,0 - 4,7) : 2 + 3,0 : 2 = 1,65 GB

  Der Wert für den zusätzlichen Speicherplatz kann nur ungefähr angegeben werden, da Abstriche für das Speichern von Protokollen und für Mehraufwand gemacht werden müssen. Die Berechnung und mögliche Größenänderung wird bei jedem Neustart ausgeführt.

- **Größe der Benutzerprofile (wenn keine separate Profilverwaltungslösung verwendet wird)**
  Zusätzlich zu dem für Anwendungen erforderlichen Speicherplatz muss auf persönlichen vDisks auch genügend Speicherplatz für das Speichern von Benutzerprofilen vorhanden sein. Schließen Sie alle nicht umgeleiteten speziellen Ordner (z. B. Dokumente und Musik) in Ihre Speicherplatzberechnungen ein. Vorhandene Profilgrößen sind in der Systemsteuerung (sysdm.cpl) verfügbar.

  Einige Profilumleitungslösungen speichern Stubdateien (Sentineldateien) anstelle echter Profildaten. Zu Beginn kann es aussehen, als würden die Profillösungen keine Daten speichern. Sie nutzen jedoch einen Dateiverzeichniseintrag pro Stubdatei im Dateisystem, was ungefähr 4 KB pro Datei ausmacht. Wenn Sie eine solche Lösung verwenden, schätzen Sie die Größe anhand der echten Profildaten und nicht basierend auf den Stubdateien.

  Unternehmensanwendungen zur Dateifreigabe, wie ShareFile und Dropbox, synchronisieren oder laden Daten möglicherweise auf die Profildatenbereiche der persönlichen vDisks von Benutzern herunter. Wenn Sie derartige Anwendungen verwenden, veranschlagen Sie genug Speicherplatz für diese Daten.

- **Mehraufwand durch die virtuelle Festplattenvorlage, die den PvD-Bestand enthält**
  Die virtuelle Festplattenvorlage enthält die PvD-Bestandsdaten (Sentineldateien, die zum Inhalt des Masterimages


© 1999-2017 Citrix Systems, Inc. All rights reserved.

gehören). Der PvD-Anwendungsbereich wird von dieser virtuellen Festplatte erstellt. Da jede Sentineldatei bzw. jeder Sentinelordner einen Dateiverzeichniseintrag im Dateisystem enthält, nimmt der Inhalt der virtuellen Festplattenvorlage PvD-Anwendungsspeicherplatz in Anspruch, bevor der Endbenutzer überhaupt eine Anwendung installiert hat. Sie können die Größe der virtuellen Festplattenvorlage bestimmten, indem Sie zum Masterimage navigieren, nachdem der Bestand aufgenommen wurde. Sie können zur ungefähren Berechnung auch die folgende Formel verwenden:

Größe der virtuellen Festplattenvorlage = (Anzahl der Dateien des Basisimage) x 4 KB

Sie ermitteln die Anzahl der Dateien und Ordner, indem Sie mit der rechten Maustaste auf das Laufwerk C: des Images der Basis-VM klicken und Eigenschaften auswählen. Beispiel: Ein Image mit 250.000 Dateien ergibt eine virtuelle Festplattenvorlage von ungefähr 1.024.000.000 Bytes (nicht ganz 1 GB). Dieser Speicherplatz ist nicht für Anwendungsinstallationen im PvD-Anwendungsbereich verfügbar.

- **Mehraufwand für PvD-Imageupdatevorgänge**
  Während PvD-Imageupdatevorgänge ausgeführt werden, muss im Stammverzeichnis der PvD (standardmäßig P:) genug Speicherplatz vorhanden sein, um die Änderungen der zwei Imageversionen mit den Änderungen, die der Benutzer an der PvD vorgenommen hat, zusammenzuführen. Normalerweise reserviert die PvD einige Hundert MB für diesen Zweck. Durch Extradaten, die im Laufwerk P: gespeichert wurden, ist jedoch möglicherweise nicht genug Speicherplatz zum Durchführen des Imageupdates vorhanden. Mit dem PvD-Poolstatistikscript (auf dem XenDesktop-Installationsmedium im Ordner "Support/Tools/Scripts") oder mit dem Überwachungstool für PvD-Imageupdates (im Ordner "Support/Tools/PvdTool") können Sie die PvD-Datenträger in einem Katalog identifizieren, für die ein Update geplant ist und die fast voll sind.

  Das Vorhandensein von Antivirenprodukten kann sich darauf auswirken, wie lange das Durchführen einer Bestandsaktualisierung oder eines Updates dauert. Die Leistung kann verbessert werden, wenn Sie CtxPvD.exe und CtxPvDSvc.exe der Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal vdisk\bin. Durch das Ausschließen dieser ausführbaren Dateien vom Antivirenscan kann die Bestandsaktualisierungs- und Imageupdateleistung um das Zehnfache beschleunigt werden.

- **Mehraufwand für unerwartete Zunahme (unerwartete Anwendungsinstallationen usw.)**
  Kalkulieren Sie zusätzlichen Speicherplatz ein (entweder eine feste Menge oder einen Prozentsatz der vDisk-Größe), um auf unerwartete Anwendungsinstallationen von Benutzern während der Bereitstellung vorbereitet zu sein.

### Konfigurieren von Größe und Zuordnung der persönlichen vDisk

Sie können den Algorithmus für die automatische Größenänderung, der die Größe der virtuellen Festplatte relativ zum Laufwerk P: festlegt, manuell anpassen, indem Sie die Ausgangsgröße der virtuellen Festplatte festlegen. Dies ist nützlich, wenn Sie beispielsweise wissen, dass Benutzer zahlreiche Anwendungen installieren werden, die nicht alle auf die virtuelle Festplatte passen werden, selbst wenn die Größe mit dem Algorithmus angepasst wurde. In dieser Situation können Sie die Ausgangsgröße des Anwendungsspeicherplatzes erhöhen, damit die vom Benutzer installierten Anwendungen genug Platz haben.

Passen Sie die Ausgangsgröße der virtuellen Festplatte am besten auf einem Masterimage an. Sie können die Größe der virtuellen Festplatte auch auf einem virtuellen Desktop anpassen, wenn ein Benutzer nicht genügend Speicherplatz für die Installation einer Anwendung hat. Sie müssen diesen Vorgang jedoch auf allen betroffenen virtuellen Desktops wiederholen, da Sie die Ausgangsgröße der virtuellen Festplatte nicht in einem bereits erstellten Katalog ändern können.

Stellen Sie sicher, dass die virtuelle Festplatte groß genug für das Speichern von Definitionsdateien von Antivirensoftware ist, da diese Dateien normalerweise sehr umfangreich sind.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Legen Sie die folgenden Registrierungsschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config fest. (Ändern Sie keine anderen Einstellungen in diesem Registrierungsschlüssel.) Alle Einstellungen müssen auf dem Masterimage angegeben werden (außer für MinimumVHDSizeInMB, was auf einer individuellen Maschine geändert werden kann). Auf dem Masterimage angegebene Einstellungen werden bei der nächsten Aktualisierung des Images angewendet.

- **MinimumVHDSizeMB**
  Gibt die Mindestgröße (in Megabyte) des Anwendungsteils (C:) der persönlichen vDisk an. Die neue Größe muss größer als die vorhandene Größe und kleiner als die Größe des Datenträgers abzüglich PvDReservedSpaceMB sein.

  Durch das Erhöhen dieses Werts wird freier Speicherplatz vom Profilteil der vDisk dem Laufwerk C: zugeteilt. Diese Einstellung wird ignoriert, wenn ein geringerer Wert als die aktuelle Größe des Laufwerks C: verwendet wird oder wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

  Standard = 2048

- **EnableDynamicResizeOfAppContainer**
  Aktiviert oder deaktiviert den Algorithmus zur dynamischen Größenänderung.
  - Bei der Einstellung auf 1 wird der Anwendungsspeicherplatz auf C: automatisch geändert, wenn der freie Speicherplatz auf C: unter 10 % fällt. Zulässige Werte sind 1 und 0. Ein Neustart muss durchgeführt werden, damit die Änderungen wirksam werden.
  - Bei der Einstellung auf 0 wird die Größe der virtuellen Festplatte basierend auf der Methode ermittelt, die in XenDesktop-Versionen vor 7.x verwendet wurde.

  Standard = 1

- **EnableUserProfileRedirection**
  Aktiviert oder deaktiviert die Umleitung des Benutzerprofils auf die vDisk.
  - Bei der Einstellung auf 1 leitet PvD das Benutzerprofil auf die vDisk um (standardmäßig auf P:). Profile werden entsprechend einem Windows-Standardprofil im Allgemeinen nach P:\Users umgeleitet. Durch die Umleitung werden die Profile beibehalten, falls der PvD-Desktop zurückgesetzt werden muss.
  - Bei der Einstellung auf 0 ist der gesamte Speicherplatz auf der vDisk, abzüglich PvDReservedSpaceMB, dem Laufwerk C: (dem Anwendungsteil der vDisk) zugewiesen, und das vDisk-Laufwerk (P:) ist im Windows Explorer ausgeblendet. Citrix empfiehlt das Deaktivieren der Umleitung durch die Einstellung auf 0, wenn Sie Citrix Profilverwaltung oder eine andere Roamingprofillösung verwenden.
    Durch diese Einstellung bleiben die Profile in C:\Users erhalten statt auf die vDisk umgeleitet zu werden, und sie ermöglicht der Roamingprofillösung das Verwalten der Profile.

    Dieser Wert stellt sicher, dass der ganze Speicherplatz auf P: Anwendungen zugewiesen ist.

    Bei einer Einstellung dieses Werts auf 0 wird davon ausgegangen, dass eine Profilverwaltungslösung eingesetzt wird. Das Deaktivieren der Profilumleitung ohne eine Roamingprofillösung einzusetzen wird nicht empfohlen, da die Profile sonst bei nachfolgenden PvD-Zurücksetzungsvorgängen gelöscht werden.

  Ändern Sie diese Einstellung nicht, wenn das Image aktualisiert wird, da sie zwar nicht den Speicherort vorhandener Profile ändert, jedoch den gesamten Speicherplatz auf der PvD dem Laufwerk C: zuweist und die PvD ausblendet.

  Konfigurieren Sie diesen Wert vor dem Bereitstellen eines Katalogs. Nach dem Bereitstellen eines Katalogs können Sie diesen Wert nicht mehr ändern.

  Wichtig: Ab XenDesktop 7.1 werden Änderungen an diesem Wert nicht angewendet, wenn Sie ein Imageupdate ausführen. Legen Sie den Wert des Schlüssels fest, wenn Sie die Kataloge erstellen, von denen die Profile erstellt werden. Sie können das Umleitungsverhalten später nicht mehr ändern.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Standard = 1

- **PercentOfPvDForApps**
  Legt die Teilung zwischen dem Anwendungsteil (C:) und dem Profilteil der vDisk fest. Dieser Wert wird beim Erstellen neuer VMs verwendet sowie während Imageupdates, wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

  Das Ändern der Einstellung PercentOfPvDForApps macht nur einen Unterschied, wenn die Einstellung EnableDynamicResizeOfAppContainer auf 0 festgelegt ist. Standardmäßig ist EnableDynamicResizeOfAppContainer auf 1 (aktiviert) festgelegt, d. h. dass der AppContainer (Laufwerk C:) nur erweitert wird, wenn er fast voll ist (d. h. dynamisch), und zwar wenn weniger als 10 % freier Speicherplatz vorhanden ist.

  Durch das Erhöhen von PercentOfPvDForApps wird nur der Gesamtspeicherplatz für die Apps erhöht. Der Speicherplatz wird jedoch nicht sofort verfügbar gemacht. Sie müssen zudem die Zuordnungsteilung im Masterimage konfigurieren, die dann beim nächsten Imageupdate angewendet wird.

  Wenn Sie bereits einen Katalog mit Maschinen mit der Einstellung 1 für EnableDynamicResizeOfAppContainer generiert haben, ändern Sie die Einstellung im Masterimage für das nächste Update auf 0 und konfigurieren Sie die entsprechende Zuordnungsteilung. Die angeforderte Teilungsgröße wird eingehalten, solange sie größer als die aktuell zugeteilte Größe des Laufwerks C ist.

  Wenn Sie komplette Kontrolle über die Speicherplatzteilung haben möchten, legen Sie den Wert auf 0 fest. Damit haben Sie die komplette Kontrolle über die Größe des Laufwerks C und die Erweiterung des Laufwerks ist nicht davon abhängig, dass ein Benutzer eine bestimmte Menge Speicherplatz unter dem Schwellenwert in Anspruch nimmt.

  Standard = 50 % (beiden Teilen wird der gleiche Speicherplatz zugeteilt)

- **PvDReservedSpaceMB**
  Legt die Größe des reservierten Speicherplatzes (in MB) auf der vDisk für das Speichern von Personal vDisk-Protokollen und anderen Daten fest.

  Wenn in Ihrer Bereitstellung XenApp 6.5 (oder eine frühere Version) und Anwendungsstreaming verwendet wird, erhöhen Sie diesen Wert um die Größe des RadeCache.

  Standard = 512

- **PvDResetUserGroup**
  Gilt nur für XenDesktop 5.6: Ermöglicht der angegebenen Gruppe von Benutzern, eine persönliche vDisk zurücksetzen. Höhere XenDesktop-Releases verwenden dafür die delegierte Administration.

Weitere Einstellungen:

- **Windows Update Service**: Stellen Sie sicher, dass im Masterimage für Windows Updates die Einstellung Never Check for Update und für den Windows Update Service die Einstellung Disabled ausgewählt ist. Falls der Windows Update Service auf der PvD ausgeführt werden muss, wird durch die Einstellung Never Check for Update verhindert, dass die Updates auf den zugeordneten Maschinen installiert werden.
  Dieser Dienst wird von Windows 8 Store benötigt, um Modern UI-Apps installieren zu können.

- **Windows Updates**: Diese schließen Updates für Internet Explorer ein und müssen auf das Masterimage angewendet werden.
- **Updates requiring restarts**: Bei auf das Masterimage angewendeten Windows Updates sind, abhängig von den im Update enthaltenen Patches, möglicherweise mehrere Neustarts erforderlich, damit die Installation vollständig ausgeführt wird. Stellen Sie vor der PvD-Bestandsaktualisierung sicher, dass Sie das Masterimage richtig neu starten,

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

damit die Installation von ausgeführten Windows Updates vollständig abgeschlossen wird.
- **Application updates**: Aktualisieren Sie Anwendungen, die auf dem Masterimage installiert sind, um Speicherplatz auf den vDisks von Benutzern zu sparen. Auf diese Weise vermeiden Sie den doppelten Aufwand, der durch das Durchführen von Updates auf den vDisks einzelner Benutzer entstehen würde.

### Überlegungen zu Anwendungen auf dem Masterimage

Es kann zu Konflikten zwischen Software und der von PvD erstellten Benutzerumgebung kommen. Zum Vermeiden von Konflikten müssen Sie die Software auf dem Masterimage (nicht auf den individuellen Maschinen) installieren. Auch wenn es keine Konflikte zwischen der Software und der Ausführung von PvD gibt, empfiehlt Citrix, sie auf dem Masterimage zu installieren.

Folgende Anwendungen müssen auf dem Masterimage installiert werden:
- Agents und Clients (z. B. System Center Configuration Manager-Agent, App-V-Client, Citrix Receiver)
- Anwendungen, die vorrangige Starttreiber installieren oder ändern
- Anwendungen, die Drucker- oder Scannersoftware bzw. -treiber installieren
- Anwendungen, die den Windows-Netzwerkstapel ändern
- VM-Tools wie VMware Tools und XenServer Tools

Folgende Anwendungen sollten auf dem Masterimage installiert werden:
- Anwendungen, die einer großen Anzahl an Benutzern zur Verfügung gestellt werden. Deaktivieren Sie für die folgenden Fälle vor der Bereitstellung die Anwendungsupdates:
  - Unternehmensanwendungen, die Volumenlizenzierung verwenden, z. B. Microsoft Office und Microsoft SQL Server
  - Gängige Anwendungen wie Adobe Reader, Firefox und Chrome
- Große Anwendungen, z. B. SQL Server, Visual Studio und Anwendungsframeworks wie .NET

Die folgenden Empfehlungen und Einschränkungen gelten für Anwendungen, die Benutzer auf Maschinen mit persönlichen vDisks installiert haben. Einige dieser Empfehlungen können nicht durchgesetzt werden, wenn Benutzer Administratorrechte haben:
- Benutzer sollten Anwendungen nicht vom Masterimage deinstallieren und dann auf ihrer persönlichen vDisk neu installieren.
- Vorsicht beim Aktualisieren oder Deinstallieren von Anwendungen auf dem Masterimage. Nachdem Sie die Version einer Anwendung auf dem Image installiert haben, installiert ein Benutzer möglicherweise eine Add-On-Anwendung (z. B. ein Plug-In), das diese Version erfordert. Im Fall einer solchen Abhängigkeit kann es nach dem Aktualisieren oder Deinstallieren der Anwendung auf dem Image beim Add-On zu einer Fehlfunktion kommen. Beispiel: Microsoft Office 2010 ist auf einem Masterimage installiert und ein Benutzer installiert Visio 2010 auf der persönlichen vDisk. Bei einem Upgrade von Office auf dem Masterimage kann die lokal installierte Visio-Anwendung unbrauchbar werden.
- Software mit Lizenzen, die von Hardware abhängig sind (entweder durch ein Dongle oder signaturbasierte Hardware), wird nicht unterstützt.

### Überlegungen zu Provisioning Services

Wenn Sie Provisioning Services mit PvD verwenden:
- Das SOAP-Dienstkonto muss zum Administratorknoten von Studio hinzugefügt werden und es muss über die Rolle "Maschinenadministrator" oder eine höhere Rolle verfügen. Dadurch wird sichergestellt, dass die PvD-Desktops in den Status "Preparing" versetzt werden, wenn die Provisioning Services (PVS) vDisk auf "Production" hochgestuft wird.
- Das Versionsverwaltungsfeature von Provisioning Services muss zum Aktualisieren der persönlichen vDisk verwendet werden. Wenn die Version auf "Production" hochgestuft wird, versetzt der SOAP-Dienst die PvD-Desktops in den Status "Preparing".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Die Größe der persönlichen vDisk sollte immer größer als der Provisioning Services-Schreibcachedatenträger sein, da Provisioning Services sonst fälschlicherweise die persönliche vDisk als Schreibcache nehmen könnte.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts (personal-vdisk-poolstats.ps1) überwachen.

Veranschlagen Sie genug Schreibcache. Bei normalem Betrieb werden die meisten Benutzerschreibvorgänge (Änderungen) von PvD erfasst und an die persönliche vDisk umgeleitet. Daher könnten Sie theoretisch die Größe des Provisioning Services-Schreibcache verringern. Wenn PvD jedoch nicht aktiv ist, z. B. während Imageupdatevorgängen, kann ein kleines Provisioning Services-Schreibcache schnell voll sein und den Absturz von Maschinen verursachen.

Citrix empfiehlt, dass Sie die Größe des Provisioning Services-Schreibcache entsprechend den Empfehlungen für Provisioning Services veranschlagen und dann Speicherplatz hinzufügen, der dem Doppelten der virtuellen Festplattenvorlage auf dem Masterimage entspricht (für Zusammenführungen). Es ist unwahrscheinlich, dass ein Zusammenführungsvorgang so viel Speicherplatz beansprucht, aber es ist möglich.

Wenn Sie mit Provisioning Services einen Katalog mit PvD-aktivierten Maschinen bereitstellen:
- Folgen Sie den Anweisungen in der Provisioning Services-Dokumentation.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Zum Aktualisieren der Provisioning Services-vDisk installieren bzw. aktualisieren Sie Anwendungen und Software und starten Sie die vDisk neu. Aktualisieren Sie dann den PvD-Bestand und fahren Sie die VM herunter. Stufen Sie anschließend die neue Version auf "Production" hoch. Die PvD-Desktops im Katalog sollten automatisch in den Zustand "Preparing" versetzt werden. Wenn dies nicht der Fall ist, prüfen Sie, ob das SOAP-Dienstkonto Maschinenadministrator- oder höhere Privilegien auf dem Controller hat.

Mit dem Testmodusfeature von Provisioning Services können Sie einen Testkatalog mit Maschinen erstellen, die ein aktualisiertes Masterimage verwenden. Wenn die Tests die Funktionsfähigkeit des Katalogs bestätigen, stufen Sie ihn auf "Production" hoch.

### Überlegungen zu den Maschinenerstellungsdiensten

Wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Katalog mit PvD-aktivierten Maschinen bereitstellen:
- Folgen Sie den Anweisungen in der XenDesktop-Dokumentation.
- Aktualisieren Sie nach dem Erstellen des Masterimages den PvD-Bestand und schalten Sie dann die VM aus (PvD funktioniert nicht ordnungsgemäß, wenn Sie die VM nicht ausschalten). Erstellen Sie einen Snapshot vom Masterimage.
- Geben Sie im Assistenten zum Erstellen von Maschinenkatalogen die Größe und den Laufwerksbuchstaben der persönlichen vDisk an.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts (personal-vdisk-poolstats.ps1) überwachen.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Wenn Sie das Masterimage aktualisieren, nehmen Sie nach dem Aktualisieren der Anwendungen und der anderen Software auf dem Image den PvD-Bestand auf und schalten Sie anschließend die VM aus. Erstellen Sie einen Snapshot vom Masterimage.
- Überprüfen Sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1", ob genügend Speicherplatz auf jeder PvD-aktivierten VM vorhanden ist, die das aktualisierte Masterimage verwendet.
- Nach dem Aktualisieren des Maschinenkatalogs werden die PvD-Desktops in den Zustand "Preparing" versetzt, während sie die Änderungen am neuen Masterimage verarbeiten. Die Desktops werden entsprechend der während des Maschinenupdates festgelegten Rolloutstrategie aktualisiert.
- Während die PvD im Zustand "Preparing" ist, überwachen Sie sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1".

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

## Ausschließen von Dateien und Ordner von vDisks

Mit Regeldateien schließen Sie Dateien und Ordner von vDisks aus. Dies ist möglich, während die persönlichen vDisks bereitgestellt werden. Die Regeldateien werden custom_*_rules.template.txt genannt und befinden sich im Ordner \config. Anmerkungen in den einzelnen Dateien erhalten zusätzliche Informationen.

## Durchführen einer Bestandsaktualisierung beim Aktualisieren eines Masterimages

Wenn Sie PvD nach einer Aktualisierung des Masterimages aktivieren, muss der Bestand des Datenträgers aktualisiert und ein neuer Snapshot erstellt werden.

Wenn Sie eine Anwendung installieren, die Binärdateien im Benutzerprofil des Administrators ablegt, ist die Anwendung nicht für Benutzer freigegebener virtueller Desktops (einschließlich solcher, die auf gepoolten Maschinenkatalogen basieren und mit PvD-Maschinenkatalogen gepoolt sind) verfügbar, da Masterimages nicht von Benutzern sondern von Administratoren verwaltet werden. Benutzer müssen solche Anwendungen selber installieren.

Es ist ratsam, nach jedem Schritt in diesem Verfahren einen Snapshot des Images zu erstellen:

1. Aktualisieren Sie das Masterimage, indem Sie auf der Maschine Anwendungen oder Betriebssystemupdates installieren und das System konfigurieren.
   Bei Masterimages, die auf Windows XP basieren und die Sie mit persönlichen vDisks bereitstellen möchten, müssen Sie sicherstellen, dass keine Dialogfelder offen sind (z. B. Meldungen zur Bestätigung von Softwareinstallationen oder Aufforderungen, nicht signierte Treiber zu verwenden). Offene Dialogfelder auf Masterimages in dieser Umgebung verhindern, dass sich der VDA beim Delivery Controller registriert. Sie können Aufforderungen für nicht signierte Treiber in der Systemsteuerung verhindern. Navigieren Sie zu "System > Hardware > Treibersignierung" und wählen Sie die Option zum Ignorieren von Warnungen.

2. Fahren Sie die Maschine herunter. Klicken Sie bei Windows 7-Maschinen auf Abbrechen, wenn Citrix Personal vDisk das Herunterfahren behindert.
3. Klicken Sie im Citrix Personal vDisk-Dialogfeld auf Bestand aktualisieren. Dieser Vorgang kann einige Minuten dauern.
   Wichtig: Wenn Sie das anschließende Herunterfahren unterbrechen (selbst wenn Sie nur eine kleine Änderung am Image vornehmen), stimmt der Bestand der persönlichen vDisk nicht mehr mit dem Masterimage überein. Dies führt dazu, dass das Personal vDisk-Feature nicht mehr funktioniert. Wenn Sie das Herunterfahren unterbrechen, müssen Sie die Maschine neu starten, herunterfahren und auf "Bestand aktualisieren" klicken, wenn Sie dazu aufgefordert werden.
4. Erstellen Sie, nachdem der Bestandvorgang die Maschine heruntergefahren hat, einen Snapshot des Masterimages.

Sie können einen Bestand in eine Netzwerkfreigabe exportieren und ihn anschließend in ein Masterimage importieren. Weitere Informationen finden Sie unter "Exportieren und Importieren eines PvD-Bestands".

## Konfigurieren von Drosselungseinstellungen für Verbindungen

Der Citrix Brokerdienst steuert den Energiezustand der Maschinen, die Desktops und Anwendungen bereitstellen. Der Brokerdienst kann mehrere Hypervisors über einen Delivery Controller steuern. Die Interaktion zwischen einem Controller und dem Hypervisor wird durch Broker-Energieaktionen gesteuert. Aktionen, die den Energiezustand einer Maschine ändern, wird eine Priorität zugewiesen und dann werden sie über einen Drosselungsmechanismus an den Hypervisor gesendet, damit es nicht zur Überlastung kommt. Die folgenden Einstellungen wirken sich auf die Drosselung aus. Diese Werte werden festgelegt, indem Sie eine Verbindung (Seite "Erweitert") in Studio bearbeiten.

Konfigurieren von Drosselungswerten für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie die Verbindung und dann im Aktionsbereich Verbindung bearbeiten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Sie können die folgenden Werte ändern:
   - **Gleichzeitige Aktionen (alle Typen)**: Das zulässige Maximum für gleichzeitig ausgeführte Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung mit dem Hypervisor angegeben. Der niedrigere der beiden Werte wird verwendet.
     Standard = 100 absolut, 20%

   - **Gleichzeitige Updates für Personal vDisk-Bestand**: Das zulässige Maximum für gleichzeitige Personal vDisk-Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung angegeben. Der niedrigere der beiden Werte wird verwendet.
     Standard = 50 absolut, 25%

     Sie kalkulieren den absoluten Wert, indem Sie den Gesamtwert für IOPS (TIOPS) bestimmen, den der Datenträger des Endbenutzers unterstützt (dies sollte vom Hersteller festgelegt sein oder berechnet werden). Veranschlagen Sie 350 IOPS pro VM (IOPS/VM), um die Anzahl der VMs zu bestimmen, die jeweils auf dem Datenträger aktiv sein können. Sie berechnen diesen Wert, indem Sie den Gesamtwert für IOPS durch IOPS/VM teilen.

     Beispiel: Wenn der Wert für den Datenträger des Endbenutzers 14.000 IOPS ist, ist die Anzahl der aktiven VMs 14.000 IOPS : 350 IOPS/VM = 40.

   - **Höchstanzahl neue Aktionen pro Minute**: Die maximale Anzahl der neuen Energieaktionen, die pro Minute an den Hypervisor gesendet werden können. Sie wird als absoluter Wert angegeben.
     Standard = 10

Identifizieren der optimalen Werte für diese Einstellungen in der Bereitstellung:

1. Messen Sie mit den Standardwerten die Reaktionszeit für das Imageupdate eines Testkatalogs. Dies ist die Differenz zwischen der Startzeit eines Imageupdates (T1) und dem Zeitpunkt, wenn der VDA auf der letzten Maschine des Katalogs beim Controller registriert wird (T2). Reaktionszeit = T2 – T1.
2. Messen Sie die Ein- und Ausgabevorgänge pro Sekunde (IOPS) auf dem Hypervisorspeicher während des Imageupdates. Diese Daten können als Benchmark für die Optimierung dienen. (Die Standardwerte sind möglicherweise die beste Einstellung. Unter Umständen erreicht das System den maximalen IOPS-Wert, sodass die Einstellungswerte herabgesetzt werden müssen.)
3. Ändern Sie den Wert für "Gleichzeitige Updates für Personal vDisk-Bestand" wie unten beschrieben und lassen Sie alle anderen Einstellungen unverändert.
   1. Erhöhen Sie den Wert um 10 und messen Sie die Reaktionszeit nach jeder Änderung. Fahren Sie fort, den Wert um 10 zu erhöhen und messen Sie das Ergebnis, bis die Reaktionszeit abnimmt oder keine Änderung mehr auftritt.
   2. Wenn durch das Erhöhen des Werts im vorherigen Schritt keine Verbesserung erzielt wurde, verringern Sie den Wert schrittweise um 10 und messen Sie die Reaktionszeit nach jeder Verringerung. Wiederholen Sie diesen Vorgang, bis sich die Reaktionszeit nicht mehr ändert oder verbessert. Dieser Wert ist wahrscheinlich der optimale Wert für die PvD-Energieaktion.
4. Wenn Sie den Einstellungswert für die PvD-Energieaktion festgelegt haben, optimieren Sie nacheinander die Werte für die gleichzeitigen Aktionen (alle Typen) und die Höchstanzahl der neuen Aktionen pro Minute. Folgen Sie den oben erläuterten Schritten (schrittweises Erhöhen und Verringern der Werte), um verschiedene Werte zu testen.

### Verwenden von Microsoft System Center Configuration Manager 2007 mit PvD

System Center Configuration Manager (Configuration Manager) 2012 erfordert keine besondere Konfiguration und kann auf die gleiche Weise wie alle anderen Anwendungen auf dem Masterimage installiert werden. Die folgenden Informationen gelten nur für System Center Configuration Manager 2007. Configuration Manager-Versionen vor Configuration Manager 2007 werden nicht unterstützt.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Führen Sie die folgenden Schritte aus, um die Configuration Manager 2007 Agent-Software in einer PvD-Umgebung zu verwenden.

1. Installieren Sie den Client-Agent auf dem Masterimage.
   1. Installieren Sie den Configuration Manager-Client auf dem Masterimage.
   2. Beenden Sie den ccmexec-Dienst (SMS-Agent) und deaktivieren Sie ihn.
   3. Löschen Sie SMS- oder Clientzertifikate wie folgt aus dem Zertifikatspeicher des lokalen Computers:
      - Gemischter Modus: Certificates (Lokaler Computer)\SMS\Certificates
      - Einheitlicher Modus
        - Certificates (Lokaler Computer)\Personal\Certificates
        - Löschen Sie das Clientzertifikat, das von Ihrer Zertifizierungsstelle ausgestellt wurde (normalerweise eine interne PKI).
   4. Löschen Sie C:\Windows\smscfg.ini oder benennen Sie die Datei um.
2. Entfernen Sie Informationen, die den Client eindeutig identifizieren.
   1. (Optional) Löschen Sie die Protokolldateien unter C:\Windows\System32\CCM\Logs oder verschieben Sie sie.
   2. Installieren Sie ggf. den Virtual Delivery Agent und nehmen Sie den PvD-Bestand auf.
   3. Fahren Sie das Masterimage herunter, erstellen Sie einen Snapshot und erstellen Sie dann mit diesem Snapshot einen Maschinenkatalog.
3. Überprüfen Sie Personal vDisk und starten Sie die Dienste. Führen Sie diese Schritte einmal auf jedem PvD-Desktop aus, nachdem er zum ersten Mal gestartet wurde. Dazu können Sie beispielsweise ein Domänen-GPO verwenden.
   - Bestätigen Sie, dass PvD aktiv ist, indem Sie prüfen, ob der Registrierungsschlüssel HKLM\Software\Citrix\personal vDisk\config\virtual vorhanden ist.
   - Stellen Sie den ccmexec-Dienst (SMS-Agent) auf "Automatic" ein und starten Sie den Dienst. Der Configuration Manager-Client kontaktiert den Configuration Manager-Server und ruft neue, eindeutige Zertifikate und GUIDs ab.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Tools

Jul 08, 2016

Mit den folgenden Tools und Hilfsprogrammen können Sie PvD-Vorgänge anpassen, vereinfachen und überwachen.

## Benutzerdefinierte Regeldateien

Mit den von PvD bereitgestellten benutzerdefinierten Regeldateien können Sie das folgende Standardverhalten von PvD-Imageupdates ändern:

- Die Sichtbarkeit von Dateien auf der PvD
- Die Art der Zusammenführung von vorgenommenen Änderungen
- Einstellungen zur Beschreibbarkeit der Dateien

Detaillierte Anweisungen zu den benutzerdefinierten Regeldateien und dem CoW-Feature finden Sie in den Kommentaren zu den Dateien, die sich unter C:\ProgramData\Citrix\personal vDisk\Config auf der Maschine befinden, auf der PvD installiert ist. Die Dateien mit dem Namen custom_* erläutern die Regeln und wie sie aktiviert werden.

## Ändern der Größe und poolstats-Skripts

Es gibt zwei Skripts zum Überwachen und Verwalten der Größe der PvDs. Sie befinden sich im Ordner "Support\Tools\Scripts" auf dem XenDesktop-Installationsmedium. Sie können auch das Überwachungstool für PvD-Imageupdates verwenden, das sich im Ordner "Support\Tools\Scripts\PvdTool" befindet. Weitere Informationen finden Sie unter http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/.

Verwenden Sie "resize-personalvdisk-pool.ps1" zum Vergrößern der PvDs in allen Desktops eines Katalogs. Die folgenden Snap-Ins oder Module für den Hypervisor müssen auf der Maschine installiert werden, auf der Studio ausgeführt wird:

- XenServer erfordert XenServerPSSnapin
- vCenter erfordert vSphere PowerCli
- System Center Virtual Machine Manager erfordert die VMM-Konsole

Mit "personal-vdisk-poolstats.ps1" können Sie den Status von Imageupdates überprüfen sowie den Speicherplatz für Anwendungen und Benutzerprofile in einer PvD-Gruppe. Führen Sie das Skript vor dem Update eines Images aus, um zu prüfen, ob Desktops genug Speicherplatz haben. Dadurch werden Fehler während des Updates verhindert. Für das Skript muss die Windows Management Instrumentation (WMI-In)-Firewall auf den PvD-Desktops aktiviert sein. Sie können die Firewall auf dem Masterimage aktivieren oder über GPO.

Wenn ein Imageupdate fehlschlägt, zeigt der Eintrag in der Spalte "Update" die Ursache an.

## Zurücksetzen des Anwendungsbereichs

Wenn ein Desktop durch die Installation einer fehlerhaften Anwendung oder aus einem anderen Grund beschädigt wird, können Sie den Anwendungsbereich der PvD auf den (leeren) Herstellerstandard zurücksetzen. Beim Zurücksetzen bleiben die Benutzerprofildaten erhalten.

Zurücksetzen des Anwendungsbereichs der PvD:

- Melden Sie sich am Desktop des Benutzers als Administrator an. Starten Sie eine Eingabeaufforderung und führen Sie den Befehl C:\Programme\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset aus.
- Navigieren Sie in Citrix Director zum Desktop des Benutzers. Klicken Sie auf Reset Personal vDisk und anschließend auf OK.

## Exportieren und Importieren eines PvD-Bestands

Der Imageupdateprozess ist ein zentraler Teil der Bereitstellung neuer Images auf PvD-Desktops und umfasst Anpassungen, damit vorhandene persönliche vDisks mit dem neuen Basisimage funktionieren. Bei Bereitstellungen, die Maschinenerstellungsdienste (MCS) verwenden, können Sie einen Bestand von einer aktiven VM auf eine Netzwerkfreigabe exportieren und dann in ein Masterimage importieren. Mit diesem Bestand auf dem Masterimage wird eine Differenz berechnet. Obwohl das Feature zum Exportieren bzw. Importieren des Bestands nicht verwendet werden muss, kann es die Leistung des Imageupdateprozesses verbessern.

Sie müssen ein Administrator sein, um das Feature zum Exportieren/Importieren des Bestands zu verwenden. Authentifizieren Sie sich für den Export/Import ggf. bei der Dateifreigabe mit "net use". Der Benutzerkontext muss auf alle für den Export/Import verwendeten Dateifreigaben zugreifen können.

- Führen Sie zum Exportieren eines Bestands den Exportbefehl als Administrator auf einer Maschine aus, auf der sich ein VDA mit aktivierter PvD befindet (Mindestversion 7.6):
  Ctxpvdsvc.exe exportinventory "<Pfad zum Exportspeicherort>"

  Die Software erkennt den Speicherort des aktuellen Bestands und exportiert den Bestand an den angegebenen Speicherort in einen Ordner mit dem Namen "ExportedPvdInventory". Hier ein Auszug aus der Befehlsausgabe:
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory \\share location\ExportedInventory Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS ... Exportin
- Zum Importieren eines zuvor exportierten Bestands führen Sie den Importbefehl als Administrator auf dem Masterimage aus:

Importieren

Führen Sie den Importbefehl als Administrator auf dem Masterimage aus.

Ctxpvdsvc.exe importinventory "<Pfad zum exportierten Bestand>"

Der <Pfad zum exportierten Bestand> muss der vollständige Pfad für die Bestandsdateien sein; in der Regel ist das <Netzwerkspeicherort\ExportedPvdInventory>.

Der Bestand wird aus dem Importspeicherort abgerufen (zuvor wurde er mit dem Befehl zum Exportieren des Bestands hierher exportiert) und in den Bestandsspeicher auf dem Masterimage importiert. Hier ein Auszug aus der Befehlsausgabe:
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory \\share location\ExportedInventory\ExportedPvdInventory Importing inventory \\share location\ExportedInventory\ExportedPv
Nach dem Exportvorgang sollte die Netzwerkfreigabe die folgenden Dateinamen enthalten. Nach dem Importvorgang sollte der Bestandsspeicher auf dem Masterimage die gleichen Dateinamen enthalten.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

### Sichern und Wiederherstellen

Wichtig: Die Skripts verschieben die PvDs nicht an einen neuen Speicherort. Diesen Vorgang müssen Sie auf eine andere Weise ausführen.
Zwei PowerShell-Skripts im Ordner "Support\Tools\Scripts" auf dem Installationsmedium des Produkts ermöglichen das Sichern und Wiederherstellen persönlicher vDisks. Mit den Skripts zum Sichern und Wiederherstellen können Sie vorhandene PvDs und Benutzerzuweisungen von einem Katalog zu einem anderen migrieren. Dies kann nützlich sein, wenn Sie den PvD-Speicher ändern müssen. Das Skript zum Sichern erstellt eine XML-Datei mit Metadaten aus einem bestehenden Katalog. Die Metadaten enthalten den aktuellen Pfad der PvDs im Speicher und die Benutzerzuweisungen zu den PvDs. Das Skript zum Wiederherstellen verwendet die XML-Datei, um die PvDs einem neuen Katalog zuzuweisen und ihnen die richtigen Benutzer zuzuordnen.
- migration-backup.ps1 zeichnet die Zuordnung zwischen jedem Benutzer und dessen persönlicher vDisk in einem Maschinenkatalog auf und speichert diese Informationen in einer XML-Datei.
- migration-restore.ps1 erstellt mit der XML-Datei den Desktop des Benutzers in einem Maschinenkatalog neu.

Vor dem Sichern und Wiederherstellen beachten Sie Folgendes:
- Die Skripts verwenden die Hypervisor-API. Daher muss das PowerShell-Snap-In des Hypervisors auf dem Controller, auf dem die Skripts ausgeführt werden, installiert sein.
- Führen Sie die Skripts von einem Speicherort aus, der Zugriff auf den Controller hat, auf dem der Maschinenkatalog erstellt wurde.
- Die Skripts werden auf folgenden Hypervisor-Plattformen unterstützt: Citrix XenServer, Microsoft Hyper-V und VMware ESX.

**Sichern eines Maschinenkatalogs**

Führen Sie ein Backup durch, wenn ein Maschinenkatalog geändert wird. Sie können ein Backup durchführen, während die Maschinen im Katalog aktiv sind.

Verwenden Sie migration-backup.ps1 zum Sichern beliebiger Maschinenkataloge, die persönliche vDisks enthalten. Das Skript fordert die Angabe des Namens des Maschinenkatalogs und der Verbindungsinformationen für den Hypervisor an. Anschließend durchläuft es sämtliche Benutzern zugewiesene Maschinen im Maschinenkatalog und speichert für jede Maschine die Zuordnung zwischen persönlichem vDisk-Speicher und dem jeweiligen Benutzer. Diese Informationen werden in einer XML-Datei gespeichert, die folgende Struktur hat:

- PvDMigration.hypervisor.Type unterstützt VMware ESX, Citrix XenServer und Microsoft Hyper-V.
- PvDMigration.PVD speichert Informationen dazu, wo die persönliche vDisk gespeichert und welchem Benutzer sie zugeordnet ist.
- PvDMigration.PVD.DiskId ist der eindeutige Bezeichner der vDisk auf dem Hypervisor, auf dem das Backup erstellt wurde.
- PvDMigration.PVD.DiskName ist der Name der VHD- bzw. VMDK-Datei.
- PvDMigration.PVD.SRName ist der Name des Speicheranbieters, wenn das Backup erstellt wurde.
- PvDMigration.PVD.SRID ist der eindeutige Bezeichner des Speicheranbieters auf dem Hypervisor, auf dem das Backup erstellt wurde.
- PvDMigration.PVD.UserName ist der Name des Benutzers, der der vDisk zugeordnet ist.
- PvDMigration.PVD.UserSid ist die SID des Benutzers, der der vDisk zugeordnet ist.
- PvDMigration.PVD.State ist der Status der vDisk. Der Status kann "backed up" oder "processed" lauten. Er lautet "backed up" nach dem ersten Backup und ändert sich in "processed", wenn die XML-Datei für eine Wiederherstellung vom Backup verwendet wurde.

**Wiederherstellen eines Maschinenkatalogs**

Beachten Sie vor dem Wiederherstellen Folgendes:
- Sie können nur einen Maschinenkatalog wiederherstellen, der dasselbe Masterimage hat wie der gesicherte Maschinenkatalog.
- Sie müssen ein neues Masterimage erstellen, indem Sie den Bestand des Masterimages aktualisieren, auf dessen Basis der gesicherte Maschinenkatalog erstellt wurde.

Stellen Sie mit migration-restore.ps1 beliebige Maschinenkataloge mit persönlichen vDisks wieder her. Das Skript erfordert folgende Eingaben:
- Während des Backups erstellte XML-Datei.
- Name des Maschinenkatalogs, der wiederhergestellt wird.
- Name des Speicherorts an dem die nicht zugewiesenen persönlichen vDisks gespeichert sind. Dies ist in der XML-Datei aufgelistet.
- Hypervisor-Verbindungsinformationen.

Das Skript migration-restore.ps1 findet alle nicht zugewiesenen Maschinen im Maschinenkatalog und weist ihnen Benutzer zu. Außerdem fügt es die persönlichen vDisks der Benutzer den Maschinen an.

**Beispielszenario 1: Wiederherstellung eines Maschinenkatalogs und seiner persönlichen vDisks mit neuen Maschinennamen**

In diesem Szenario werden ein ganzer Maschinenkatalog und die persönlichen vDisks, die den enthaltenen Maschinen angefügt sind, wiederhergestellt. Die Maschinen erhalten neue Namen. Dies kann auftreten, wenn der Hypervisor oder ein Speicherhost ausgefallen ist oder wenn Benutzer in eine neue Infrastruktur migriert werden.
1. Führen Sie migration-backup.ps1 aus, um die Zuweisung zwischen Benutzern und persönlichen vDisks in der XML-Datei aufzuzeichnen.
2. Verschieben oder sammeln Sie mit einer Backuplösung die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog auf einen Datenträger:
   - VMware ESX oder Microsoft Hyper-V: Persönliche vDisks sind in dem vom Controller festgelegten Speicher in einem Ordner, der den Namen der Maschine enthält, dem die vDisk angefügt ist.
   - Citrix XenServer: Persönliche vDisks sind im Stamm des vom Controller festgelegten Speichers. Der Name jeder vDisk ist eine GUID.
3. Stellen Sie die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog mit einer Speicherbackuplösung wieder her:
   - ESX oder Hyper-V: Platzieren Sie die vDisks in einen neuen Ordner auf der neuen Speicherressource. Alternativ können Sie die vDisks im ursprünglichen Pfad auf der neuen Speicherressource lassen.
   - XenServer: Platzieren Sie die vDisks im Stamm der neuen Speicherressource.
4. Erstellen Sie einen Provisioning Services-vDisk- oder Maschinenerstellungsdienste-Snapshot des Masterimages, mit dem Sie den ausgefallenen Maschinenkatalog erstellt haben.
5. Führen Sie Bestand aktualisieren über das Startmenü auf der vDisk oder dem Snapshot aus.
6. Erstellen Sie den Maschinenkatalog in Studio neu und verwenden Sie dabei eine andere Benennungskonvention als für den ausgefallenen ursprünglichen Maschinenkatalog. Dadurch wird ein Katalog neuer Maschinen mit jeweils einer neuen persönlichen vDisk erstellt, die die Sitedatenbank erkennt.
7. Stellen Sie sicher, dass der neu erstellte Maschinenkatalog der richtigen Bereitstellungsgruppe zugewiesen ist.
8. Stellen Sie sicher, dass die Bereitstellungsgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
9. Bearbeiten Sie die vom Backupskript generierte XML-Datei:
   - ESX oder Hyper-V: Wenn Sie vDisks in Schritt 3 in einem neuen Ordner auf der neuen Speicherressource wiederhergestellt haben, ersetzen Sie für jeden PVD-Abschnitt in der Datei den Ordnernamen in DiskName durch den Speicherort der wiederhergestellten vDisks. Wenn Sie die vDisks im ursprünglichen Pfad im neuen Speicher wiederhergestellt haben, überspringen Sie diesen Schritt.
   - XenServer: Überspringen Sie diesen Schritt.
10. Führen Sie auf dem Controller migration-restore.ps1 aus und geben Sie den Namen der XML-Datei und den Speicherort der gesicherten vDisks an.

**Beispielszenario 2: Wiederherstellung eines Maschinenkatalogs und seiner persönlichen vDisks unter Wiederverwenden der bestehenden Maschinennamen**

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

In diesem Szenario werden ein ganzer Maschinenkatalog und die persönlichen vDisks, die den enthaltenen Maschinen angefügt sind, wiederhergestellt. Die bestehenden Namen der (ausgefallenen) Maschinen werden wiederverwendet. Dieses Szenario ist möglich, wenn der Hypervisor oder ein Speicherhost ausgefallen ist.

1. Führen Sie migration-backup.ps1 aus, um die Zuordnung zwischen Benutzern und persönlichen vDisks aufzuzeichnen.
2. Verschieben oder sammeln Sie mit einer Backuplösung die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog auf einen Datenträger:
   - ESX oder Hyper-V: Persönliche vDisks sind in dem vom Controller festgelegten Speicher in einem Ordner, der den Namen der Maschine enthält, dem die vDisk angefügt ist.
   - XenServer: Persönliche vDisks sind im Stamm des vom Controller festgelegten Speichers. Der Name jeder vDisk ist eine GUID.
3. Stellen Sie die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog mit einer Speicherbackuplösung wieder her:
   - ESX oder Hyper-V: Platzieren Sie die vDisks in einen neuen Ordner auf der neuen Speicherressource.
   - XenServer: Platzieren Sie die vDisks im Stamm der neuen Speicherressource.
4. Erstellen Sie einen Provisioning Services-vDisk- oder Maschinenerstellungsdienste-Snapshot des Masterimages, mit dem Sie den ausgefallenen Maschinenkatalog erstellt haben.
5. Führen Sie Bestand aktualisieren über das Startmenü auf der vDisk oder dem Snapshot aus.
6. Erstellen Sie den Maschinenkatalog in Studio neu und verwenden Sie dabei die gleiche Benennungskonvention wie für den ausgefallenen Maschinenkatalog. Dadurch wird ein Katalog neuer Maschinen mit jeweils einer neuen persönlichen vDisk erstellt, die die Sitedatenbank erkennt.
7. Stellen Sie sicher, dass der neu erstellte Maschinenkatalog der richtigen Bereitstellungsgruppe zugewiesen ist.
8. Stellen Sie sicher, dass die Desktopgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
9. Bearbeiten Sie die vom Backupskript generierte XML-Datei:
   - ESX oder Hyper-V: Ersetzen Sie für jeden PVD-Abschnitt in der Datei den Ordnernamen in DiskName durch den Speicherort der wiederhergestellten vDisks.
   - XenServer: Überspringen Sie diesen Schritt.
10. Führen Sie das Skript migration-restore.ps1 auf dem Controller aus und verwenden Sie die geänderte XML-Datei als Eingabe. Das Skript fügt die vDisks an, ohne sie zu verschieben.
11. Überprüfen Sie, ob die Benutzerdaten erfolgreich wiederhergestellt wurden.

**Beispielszenario 3: Wiederherstellung einer Teilmenge persönlicher vDisks in einem Maschinenkatalog**

In diesem Szenario sind nur einige der persönlichen vDisks in einem Maschinenkatalog ausgefallen und werden wiederhergestellt. Die virtuellen Maschinen im Katalog sind nicht ausgefallen.

1. Führen Sie migration-backup.ps1 aus, um die Zuweisung zwischen Benutzern und persönlichen vDisks in der XML-Datei aufzuzeichnen.
2. Die XML-Datei enthält einen PVD-Abschnitt für jeden Benutzer im Maschinenkatalog. Entfernen Sie alle Benutzer, deren persönliche vDisks nicht wiederhergestellt werden müssen, und die zugehörigen Abschnitte aus der Datei.
3. Stellen Sie die persönlichen vDisks mit einer Backuplösung aus dem ursprünglichen Maschinenkatalog wie in einem der anderen Szenarios beschrieben wieder her:
   - Zum Verwenden neuer Maschinennamen folgen Sie Beispielszenario 1.
   - Zur Erhalten bestehenden Maschinennamen folgen Sie Beispielszenario 2.
4. Stellen Sie sicher, dass der Katalog genügend nicht zugewiesene Maschinen hat. Fügen Sie, falls erforderlich, Maschinen hinzu. Sie benötigen eine neue Maschine für jeden Benutzer, dessen vDisk Sie wiederherstellen möchten.
5. Stellen Sie sicher, dass die Desktopgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
6. Führen Sie auf dem Controller migration-restore.ps1 mit der geänderten XML-Datei als Eingabe aus.
7. Überprüfen Sie, ob die Benutzerdaten erfolgreich wiederhergestellt wurden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anzeigen, Meldungen und Problembehandlung

Jul 08, 2016

Wenn Sie in Studio eine PvD-aktivierte Maschine in einem Maschinenkatalog auswählen, können Sie auf der Registerkarte "PvD" den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Folgende Zustandsanzeigen sind während eines Imageupdates möglich: Ready, Preparing, Waiting, Failed und Requested.

Ein Imageupdate kann aus verschiedenen Gründen fehlschlagen, einschließlich zu wenig Speicherplatz oder weil ein Desktop die PvD nicht rechtzeitig findet. Wenn Studio angibt, dass ein Imageupdate fehlgeschlagen ist, wird ein Fehlercode mit beschreibendem Text angezeigt, um Sie bei der Problembehandlung zu unterstützen. Verwenden Sie das Überwachungstool für PvD-Imageupdates oder das Skript "personal-vdisk-poolstats.ps1" zum Überwachen des Imageupdatevorgangs und um Fehlercodes für das Problem zu erhalten.

Wenn ein Imageupdate fehlschlägt, finden Sie in den folgenden Protokolldateien weitere Informationen zur Problembehandlung:

- PvD-Dienstprotokoll: C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD-Aktivierungsprotokoll: P:\PVDLOGS\PvDActivation.log.txt

Der aktuelle Inhalt ist am Ende der Protokolldatei.

## Fehlermeldungen: 7.6 und höher

Die folgenden Fehler gelten nur für PvD Version 7.6 und höher:

- **Ein interner Fehler ist aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen. Fehlercode% Disk (% s)**
  Dieser Code gilt für alle nicht kategorisierten Fehler und hat daher keinen numerischen Wert. Alle unerwarteten Fehler während der Bestandserstellung oder dem Update von Personal vDisk sind mit diesem Fehlercode gekennzeichnet.
  - Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.
  - Wenn dieser Fehler während der Aktualisierung des Katalogs auftritt, führen Sie ein Rollback des Katalogs auf die vorherige Version des Masterimages aus.
- **Die Regeldateien enthalten Syntaxfehler. Weitere Informationen finden Sie in den Protokollen.**
  Fehlercode 2. Die Regeldatei enthält Syntaxfehler. Die Personal vDisk-Protokolldatei enthält den Namen der Regeldatei und die Zeile, in der der Syntaxfehler gefunden wurde. Beheben Sie den Syntaxfehler in der Regeldatei und wiederholen Sie den Vorgang.
- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist beschädigt oder nicht lesbar.**
  Fehlercode 3. Der letzte Bestand ist in "UserData.V2.vhd" unter "\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST" gespeichert. Stellen Sie den Bestand entsprechend der letzten Version des Masterimages wieder her, indem Sie den Ordner "VER-LAST" von einer funktionierenden PvD-Maschine importieren, die der vorherigen Version des Masterimages zugeordnet ist.
- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist eine höhere Version.**
  Fehlercode 4. Die Ursache ist eine PvD-Versionsinkompatibilität zwischen dem letzten Masterimage und dem aktuellen Masterimage. Installieren Sie die aktuelle Version von Personal vDisk auf dem Masterimage und aktualisieren Sie den Katalog erneut.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Änderungsjournalüberlauf erkannt.**
  Fehlercode 5. Ein USN-Journalüberlauf wurde durch zahlreiche Änderungen am Masterimage während der Bestandserstellung verursacht. Wenn dieses Problem nach mehreren Versuchen weiterhin auftritt, ermitteln Sie mit Process Monitor, ob die Drittanbietersoftware während der Erstellung des Bestands zahlreiche Dateien erstellt oder löscht.

- **Personal vDisk konnte keinen an das System angeschlossenen Datenträger zum Speichern von Benutzerdaten finden.**
  Fehlercode 6. Überprüfen Sie zunächst, ob die PvD über die Hypervisor-Konsole mit der VM verbunden ist. Dieser Fehler tritt häufig auf, weil Software zum Vermeiden von Datenverlust den Zugriff auf die PvD verhindert. Wenn die PvD mit der VM verbunden ist, fügen Sie eine Ausnahme für den verbundenen Datenträger in der Konfiguration der Software zum Vermeiden von Datenverlust hinzu.

- **Das System wurde nach der Installation noch nicht neu gestartet. Starten Sie es neu, damit die Änderungen übernommen werden.**
  Fehlercode 7. Starten Sie den Desktop neu und wiederholen Sie den Vorgang.

- **Beschädigte Installation. Installieren Sie Personal vDisk neu.**
  Fehlercode 8. Installieren Sie Personal vDisk neu und versuchen Sie es noch einmal.

- **Der Personal vDisk-Bestand ist nicht auf dem aktuellen Stand. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal.**
  Fehlercode 9. Der Personal vDisk-Bestand wurde vor dem Herunterfahren des Desktops nicht auf dem Masterimages aktualisiert. Starten Sie das Masterimage neu und fahren Sie den Desktop mit der Option "Persönliche vDisk aktualisieren" herunter. Erstellen Sie dann einen neuen Snapshot und aktualisieren Sie damit den Katalog.

- **Beim Start von Personal vDisk ist ein interner Fehler aufgetreten Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**
  Fehlercode 10. Die Ursache ist möglicherweise, dass der PvD-Treiber aufgrund eines internen Fehlers oder Beschädigung der persönlichen vDisk keine Virtualisierungssitzung starten kann. Starten Sie den Desktop über den Controller neu. Wenn das Problem weiterhin auftritt, sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk-Timeout bei dem Versuch, ein Speichermedium für die Personalisierungseinstellungen der Benutzer zu finden.**
  Fehlercode 11. Dieser Fehler tritt auf, wenn der PvD-Treiber den PvD-Datenträger nicht innerhalb von 30 Sekunden nach dem Neustart findet. Die Ursache ist normalerweise ein nicht unterstützter SCSI-Controllertyp oder Speicherlatenz. Wenn dieses Problem bei allen Desktops im Katalog auftritt, ändern Sie den der Vorlagen-VM bzw. Master-VM zugeordneten SCSI-Controllertyp in einen Typ, der von Personal vDisk unterstützt wird. Wenn dieses Problem nur bei einigen Desktops im Katalog auftritt, wird dies möglicherweise durch Speicherlatenz-Spitzen verursacht, weil zahlreiche Desktops gleichzeitig gestartet werden. Beschränken Sie die Einstellung für die maximale Anzahl aktiver Energieaktionen für die Hostverbindung.

- **Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Starten Sie die Maschine neu.**
  Fehlercode 12. Möglicherweise kann ein Desktop bei aktivierter PvD den Startvorgang nicht abschließen. Starten Sie den Desktop neu. Wenn das Problem weiterhin auftritt, beobachten Sie den Startvorgang des Desktops über die Hypervisor-Konsole und prüfen Sie, ob der Desktop abstürzt. Wenn ein Desktop während des Starts abstürzt, stellen Sie die PvD aus einem Backup (wenn vorhanden) wieder her oder setzen Sie die PvD zurück.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Der zum Bereitstellen von Personal vDisk angegebene Laufwerksbuchstabe ist nicht verfügbar.**
  Fehlercode 13. Die Ursache ist möglicherweise, dass Personal vDisk den PvD-Datenträger nicht über das vom Administrator angegebene Laufwerk bereitstellen kann. Der PvD-Datenträger kann nicht bereitgestellt werden, wenn der Laufwerksbuchstabe bereits von anderer Hardware verwendet wird. Wählen Sie einen anderen Buchstaben als Bereitstellungspunkt für die persönliche vDisk aus.

- **Fehler beim Installieren von Personal vDisk-Kernelmodustreibern.**
  Fehlercode 14. Personal vDisk installiert Treiber während der ersten Bestandsaktualisierung nach der Installation. Einige Antivirenprodukte verhindern die Installation von Treibern außerhalb eines Installationsprogramms. Deaktivieren Sie vorübergehend den in Echtzeit ausgeführten Antivirenscan oder fügen Sie der Antivirensoftware während der ersten Bestandserstellung Ausnahmen für die PvD-Treiber hinzu.

- **Es konnte kein Snapshot des Systemvolumes erstellt werden. Stellen Sie sicher, dass der Volumeschattenkopie-Dienst aktiviert ist.**
  Fehlercode 15. Dieser Fehler kann auftreten, weil der Volumeschattenkopie-Dienst deaktiviert ist. Aktivieren Sie den Volumeschattenkopie-Dienst und versuchen Sie noch einmal, den Bestand aufzunehmen.

- **Fehler beim Aktivieren des Änderungsjournals. Warten Sie einige Minuten und versuchen Sie es noch einmal.**
  Fehlercode 16. Personal vDisk verwendet das Änderungsjournal für das Verfolgen von Änderungen am Masterimage. Wenn PvD bei einer Bestandsaktualisierung erkennt, dass das Änderungsjournal deaktiviert ist, versucht PvD, es zu aktivieren. Der Fehler tritt auf, wenn die Aktivierung fehlschlägt. Warten Sie ein paar Minuten und versuchen Sie es noch einmal.

- **Nicht genügend freier Speicherplatz auf dem Systemvolume.**
  Fehlercode 17. Für das Imageupdate ist nicht genug freier Speicherplatz auf dem Laufwerk C des Desktops vorhanden. Erweitern Sie das Systemvolume oder entfernen Sie nicht verwendete Dateien vom Systemvolume. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Es ist nicht genügend freier Speicherplatz im Personal vDisk-Speicher. Erweitern Sie den Personal vDisk-Speicher.**
  Fehlercode 18. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während des Imageupdatevorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Der Personal vDisk-Speicher ist überbucht. Erweitern Sie den Personal vDisk-Speicher.**
  Fehlercode 19. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk für die in vollem Umfang bereitgestellte "UserData.V2.vhd" vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

- **Fehlerhafte Systemregistrierung.**
  Fehlercode 20. Die Systemregistrierung ist beschädigt, nicht lesbar oder fehlt. Setzen Sie die persönliche vDisk zurück oder stellen Sie sie von einem früheren Backup wieder her.

- **Beim Zurücksetzen von Personal vDisk ist ein interner Fehler aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**
  Fehlercode 21. Dieser Code gilt für alle Fehler, die beim Zurücksetzen von Personal vDisk auftreten. Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk konnte nicht zurückgesetzt werden, da nicht genügend freier Speicherplatz im persönlichen vDisk-Speicher ist.**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Fehlercode 22. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während eines Zurücksetzungsvorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

### Fehlermeldungen: vor Version 7.6

Die folgenden Fehler gelten nur für PvD 7.x-Versionen vor Version 7.6:

- **Start fehlgeschlagen. Personal vDisk konnte kein Speichermedium für die Personalisierungseinstellungen der Benutzer finden.**
  Die PvD-Software konnte die Personal vDisk (standardmäßig Laufwerk P:) nicht finden oder nicht als den vom Administrator bei der Erstellung des Katalogs ausgewählten Bereitstellungspunkt bereitstellen.
  - Prüfen Sie, ob Sie im PvD-Dienstprotokoll den folgenden Eintrag finden: "PvD 1 status --> 18:183".
  - Wenn Sie eine ältere Version als PvD Version 5.6.12 verwenden, löst ein Upgrade auf die aktuelle Version das Problem.
  - Wenn Sie Version 5.6.12 oder höher verwenden, prüfen Sie mit dem Datenträgerverwaltungstool (diskmgmt.msc), ob das Laufwerk P: als nicht bereitgestelltes Volume vorhanden ist. Wenn es vorhanden ist, führen Sie chkdsk auf dem Volume aus, um festzustellen, ob es fehlerhaft ist. Versuchen Sie, das Volume mit chkdsk wiederherzustellen.
- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk. Weitere Informationen ... Statuscode: 7, Fehlercode: 0x70**
  Statuscode 7 bedeutet, dass ein Fehler beim Update der PvD aufgetreten ist. Es gibt die folgenden Fehler:

| Fehlercode | Beschreibung |
|---|---|
| 0x20000001 | Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte. |
| 0x20000004 | Unzureichende Privilegien zum Aktualisieren der PvD. |
| 0x20000006 | Fehler beim Laden der Struktur aus dem PvD-Image oder dem PvD-Bestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands. |
| 0x20000007 | Fehler beim Laden des Dateisystembestands, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands. |
| 0x20000009 | Fehler beim Öffnen der Datei mit dem Dateisystembestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands. |
| 0x2000000B | Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte. |
| 0x20000010 | Fehler beim Laden des Vergleichspakets. |
| 0x20000011 | Regeldateien fehlen. |
| 0x20000021 | Fehlerhafter PvD-Bestand. |
| 0x20000027 | Der Katalog "MojoControl.dat" ist fehlerhaft. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Fehlercode | Beschreibung |
|---|---|
| 0x2000002B | PvD-Bestand fehlerhaft oder fehlt. |
| 0x2000002F | Fehler beim Registrieren des vom Benutzer installierten MOF beim Imageupdate. Lösung: Upgrade auf Version 5.6.12. |
| 0x20000032 | Suchen Sie in PvDactivation.log.txt nach dem letzten Eintrag mit einem Win32-Fehlercode. |
| 0x20 | Fehler beim Bereitstellen des Anwendungscontainers für Imageupdate. Lösung: Upgrade auf Version 5.6.12. |
| 0x70 | Nicht genügend Speicherplatz auf dem Datenträger. |

- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk [oder Personal vDisk hat einen internen Fehler festgestellt]. Weitere Informationen... Statuscode 20, Fehlercode 0x20000028**
  Die persönliche vDisk wurde gefunden, eine PvD-Sitzung konnte jedoch nicht erstellt werden.

  Sammeln Sie die Protokolle und prüfen Sie das Protokoll "SysVol-IvmSupervisor.log" auf Sitzungserstellungsfehler:
  1. Suchen Sie nach dem Protokolleintrag "IvmpNativeSessionCreate: failed to create native session, status XXXXX".
  2. Wenn der Status 0xc00002cf ist, können Sie das Problem lösen, indem Sie eine neue Version des Masterimages zum Katalog hinzufügen. Dieser Statuscode bedeutet, dass ein USN-Journalüberlauf aufgrund zahlreicher Änderungen nach einer Bestandsaktualisierung aufgetreten ist.
  3. Starten Sie den betroffenen virtuellen Desktop neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Citrix.
- **Start fehlgeschlagen. Citrix Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Wählen Sie "Noch einmal versuchen". Wenn das Problem weiterhin besteht, wenden Sie sich an den Systemadministrator.**
  Die gepoolte VM kann den Start nicht ausführen, solange die PvD aktiviert ist. Stellen Sie zuerst fest, warum der Start nicht ausgeführt werden kann. Eine mögliche Ursache ist die Anzeige eines blauen Bildschirms aus einem der folgenden Gründe:
  - Ein nicht kompatibles Antivirenprodukt ist auf dem Masterimage vorhanden, z. B. alte Versionen von Trend Micro.
  - Der Benutzer hat Software installiert, die mit PvD nicht kompatibel ist. Dies ist zwar unwahrscheinlich, aber Sie können es überprüfen, indem Sie dem Katalog eine neue Maschine hinzufügen und testen, ob sie neu startet.
  - Das PvD-Image ist fehlerhaft. Dieser Fehler wurde in Version 5.6.5 beobachtet.

  Prüfen, ob die gepoolte VM einen blauen Bildschirm anzeigt oder ob sie vorzeitig neu startet:
  - Melden Sie sich bei der Maschine über die Hypervisor-Konsole an.
  - Klicken Sie auf Noch einmal versuchen und warten Sie, bis die Maschine heruntergefahren ist.
  - Starten Sie die Maschine über Studio.
  - Beobachten Sie die Maschinenkonsole während des Starts mit der Hypervisor-Konsole.

  Weitere Problembehandlungsschritte:
  - Senden Sie das Speicherabbild der Maschine, die den blauen Bildschirm hat, zur Analyse an den technischen Support von Citrix.
  - Prüfen Sie auch die der PvD zugeordneten Ereignisprotokolle auf Fehler:
    1. Stellen Sie "UserData.V2.vhd" (im Stamm von Laufwerk P:) mithilfe von DiskMgmt.msc bereit, indem Sie auf Aktion > Virtuelle Festplatte anfügen klicken.
    2. Starten Sie "Eventvwr.msc".
    3. Öffnen Sie das Systemereignisprotokoll (Windows\System32\winevt\logs\system.evtx) aus UserData.V2.vhd, indem


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.

4. Öffnen Sie das Anwendungsereignisprotokoll (Windows\System32\winevt\logs\application.evtx) aus UserData.V2.vhd, indem Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.

- **Die persönliche vDisk kann nicht gestartet werden. Die persönliche vDisk konnte nicht gestartet werden, da der Bestand nicht aktualisiert worden ist. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal. Statuscode: 15, Fehlercode: 0x0**
  Der Administrator hat beim Erstellen oder Aktualisieren des PvD-Katalogs den falschen Snapshot ausgewählt (d. h. das Masterimage wurde beim Erstellen des Snapshots nicht mit Persönliche vDisk aktualisieren heruntergefahren).

## Von Personal vDisk protokollierte Ereignisse

Wenn Personal vDisk nicht aktiviert ist, können Sie die folgenden Ereignisse in der Windows-Ereignisanzeige anzeigen. Wählen Sie im linken Bereich den Knoten Anwendungen, die Quelle im rechten Bereich ist Citrix Personal vDisk. Wenn Personal vDisk aktiviert ist, werden diese Ereignisse nicht angezeigt.

Die Ereignis-ID 1 bedeutet, dass es sich um eine Informationsmeldung handelt. ID 2 steht für einen Fehler. Möglicherweise werden nicht alle Ereignisse in jeder Personal vDisk-Version verwendet.

| Ereignis-ID | Beschreibung |
|---|---|
| 1 | Status von Personal vDisk: Bestandsaktualisierung gestartet. |
| 1 | Status von Personal vDisk: Bestandsaktualisierung abgeschlossen. GUID: %s. |
| 1 | Status von Personal vDisk: Imageupdate gestartet. |
| 1 | Status von Personal vDisk: Imageupdate abgeschlossen. |
| 1 | Zurücksetzen wird durchgeführt. |
| 1 | OK. |
| 2 | Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen mit: %s. |
| 2 | Status von Personal vDisk: Imageupdate fehlgeschlagen mit: %s. |
| 2 | Status von Personal vDisk: Imageupdate fehlgeschlagen, interner Fehler. |
| 2 | Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen: interner Fehler. |
| 2 | Personal vDisk wurde unsachgemäß beendet und daher deaktiviert. |
| 2 | Imageupdate fehlgeschlagen. Fehlercode %d. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Ereignis-ID | Beschreibung |
|---|---|
| 2 | Personal vDisk hat einen internen Fehler festgestellt. Statuscode[%d] Fehlercode[0x%X]. |
| 2 | Zurücksetzung von Personal vDisk fehlgeschlagen. |
| 2 | Datenträger zum Speichern der angepassten Benutzereinstellungen kann nicht gefunden werden. |
| 2 | Zum Erstellen eines Personal vDisk-Containers ist nicht genug Speicherplatz auf dem Datenträger vorhanden. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Entfernen von Komponenten

Jul 08, 2016

Zum Entfernen von Komponenten empfiehlt Citrix die Verwendung der Windows-Funktion zum Entfernen oder Ändern von Programmen. Alternativ können Sie Komponenten über die Befehlszeile oder mit einem auf dem Installationsmedium enthaltenen Skript entfernen.

Beim Entfernen von Komponenten werden keine Voraussetzungen entfernt und keine Firewalleinstellungen geändert. Wenn Sie einen Controller entfernen, werden die SQL-Serversoftware und die Datenbanken nicht entfernt.

Bevor Sie einen Controller entfernen, müssen Sie ihn aus der Site entfernen. Vor dem Entfernen von Studio oder Director empfiehlt Citrix das Schließen dieser Anwendungen.

Wenn Sie einen Controller von einer früheren Bereitstellung mit dem Web Interface aktualisiert haben, müssen Sie zuerst die Webinterface-Komponente separat entfernen. Das Webinterface kann nicht mit dem Installationsprogramm entfernt werden.

## Entfernen von Komponenten mit der Windows-Funktion zum Entfernen oder Ändern von Programmen

Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:

- Zum Entfernen eines Controllers, von Studio, Director, eines Lizenzservers oder von StoreFront wählen Sie Citrix XenApp oder Citrix XenDesktop , klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
  Alternativ können Sie StoreFront entfernen, indem Sie mit der rechten Maustaste auf Citrix StoreFront klicken und dann Deinstallieren auswählen.
- Klicken Sie zum Entfernen eines VDAs auf Citrix Virtual Delivery Agent , klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
- Zum Entfernen des universellen Druckservers wählen Sie Citrix Universeller Druckserver, klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren.

## Entfernen von Kernkomponenten über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl XenDesktopServerSetup.exe aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove" und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl wird beispielsweise Studio entfernt:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

## Entfernen eines VDAs über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl XenDesktopServerSetup.exe aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove" und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl werden beispielsweise der VDA und Receiver entfernt:
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
Informationen zum Entfernen von VDAs mit einem Skript in Active Directory finden Sie unter Installieren oder Entfernen von Virtual Delivery Agents mit Skripts.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Upgrades und Migration

Jul 08, 2016

## Upgrades

Bei Upgrades werden Bereitstellungen auf die neuesten Komponentenversionen aktualisiert, ohne dass neue Maschinen oder Sites erstellt werden müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet. Sie können ein Upgrade folgender Versionen durchführen:

- Von XenDesktop 5 (oder einer höheren Version) auf die aktuelle XenDesktop-Version
- Von XenApp 7.5 auf die aktuelle XenApp-Version

Sie können auch einen XenApp 6.5-Workerserver auf einen aktuellen XenApp 7.6 für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5.

Aktualisieren einer XenDesktop 5-Farm (oder höher) oder einer XenApp 7.5-Site

1. Führen Sie das Installationsprogramm auf den Maschinen aus, auf denen die Kernkomponenten und VDAs installiert sind. Die Software ermittelt, ob ein Upgrade zur Verfügung steht und installiert die aktuelle Version.
2. Verwenden Sie das aktualisierte Studio zum Aktualisieren der Datenbank und der Site.

Weitere Informationen finden Sie unter Upgrade einer Bereitstellung.

Weitere Informationen zur Installation von Hotfixes für Controller finden Sie im Knowledge Center-Artikel CTX201988.

Aktualisieren eines XenApp 6.5-Workerserver auf einen aktuellen VDA:

1. Führen Sie das Produktinstallationsprogramm auf dem XenApp 6.5-Workerserver aus. Die Software entfernt den Server aus der XenApp 6.5-Farm, dann wird die XenApp 6.5-Software entfernt und ein aktueller VDA für Windows-Serverbetriebssysteme wird installiert.
2. Fügen Sie den Server nach dem Upgrade den Maschinenkatalogen und Bereitstellungsgruppen der aktuellen Site hinzu.

Weitere Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

## Migration

Durch Migration werden Daten von einer früheren Bereitstellung in die aktuelle Version verschoben. Sie können sowohl eine XenApp 6.5- als auch eine XenDesktop 4-Bereitstellung migrieren. Eine Migration umfasst die Installation aktueller Komponenten und das Erstellen einer neuen Site, das Exportieren der Daten aus der älteren Farm und dann das Importieren der Daten in die neue Site.

Migrieren von XenApp 6.5

1. Installieren Sie die Kernkomponenten und erstellen Sie eine neue XenApp-Site.
2. Exportieren Sie Richtlinien- und/oder Farmdaten vom XenApp 6.5-Controller mit PowerShell-Cmdlets in XML-Dateien. Sie können den Inhalt der XML-Dateien bearbeiten, um die zu importierenden Informationen anzupassen.
3. Importieren Sie in der neuen Site die Richtlinien- und/oder Anwendungsdaten mit PowerShell-Cmdlets und den XML-Dateien.
4. Schließen Sie die nach der Migration erforderlichen Schritte für die neue Site ab.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Migrieren von XenDesktop 4


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Installieren Sie die Kernkomponenten und erstellen Sie eine neue XenDesktop-Site.
2. Exportieren Sie mit dem Exportbefehl die Farmdaten von der XenDesktop 4-Farm in eine XML-Datei. Sie können den Inhalt der XML-Dateien bearbeiten, um die zu importierenden Informationen anzupassen.
3. Importieren Sie in der neuen Site die Farmdaten mit dem Importbefehl und der XML-Datei.
4. Schließen Sie die nach der Migration erforderlichen Schritte für die neue Site ab.

Weitere Informationen finden Sie unter Migrieren von XenDesktop 4.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Upgrade einer Bereitstellung

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Aktualisierbare Produktkomponenten
- Anforderungen, Einschränkungen und Vorbereitung
- Hinweise zu heterogenen Umgebungen
- VDAs auf Maschinen mit Windows XP oder Windows Vista
- VDAs auf Maschinen mit Windows 8.x oder Windows 7
- Unterstützung gemischter VDAs
- Aktualisierungsreihenfolge


# Einführung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet. Sie können ein Upgrade folgender Versionen durchführen:

- Von XenDesktop 5 (oder einer höheren Version) auf die neueste freigegebene ("aktuelle") XenDesktop-Version
- Von XenApp 7.5 (oder einer höheren Version) auf die neueste freigegebene ("aktuelle") XenApp-Version

Sie können mit dem aktuellen XenApp-Installationsprogramm auch einen XenApp 6.5-Workerserver auf einen aktuellen VDA für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5. Weitere Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

Zum Starten eines Upgrades führen Sie das Installationsprogramm in der neuen Version aus, um zuvor installierte Kernkomponenten (Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver) sowie Virtual Delivery Agents zu aktualisieren. Das Installationsprogramm ermittelt, welche Komponenten ein Upgrade erfordern und startet dann das Upgrade auf Ihren Befehl hin. Nach dem Upgrade der Komponenten verwenden Sie die neu aktualisierte Version von Studio zum Durchführen des Upgrades der Site-Datenbank und der Site.

Im vorliegenden Dokument bezieht sich "Produkt", sofern nicht anders angegeben, auf XenApp 7.x oder XenDesktop 7.x.

# Aktualisierbare Produktkomponenten

Mit dem Produktinstallationsprogramm und Studio können Sie folgende Komponenten aktualisieren:

- Delivery Controller 5 oder höher
- VDA 5.0 SP1 oder höher
  - Im Gegensatz zu früheren VDA-Releases müssen Sie für das Upgrade der VDAs das Produktinstallationsprogramm verwenden, MSI-Dateien können nicht verwendet werden.
  - Wenn das Installationsprogramm auf der Maschine Receiver für Windows erkennt (Receiver.exe), erfolgt ein Upgrade auf die Receiver-Version auf dem Installationsmedium des Produkts.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

  - VDA 5.0 SP1 bis 7.8: Wenn das Installationsprogramm Receiver für Windows Enterprise (CitrixReceiverEnterprise.exe) auf der Maschine erkennt, erfolgt ein Upgrade auf Receiver für Windows Enterprise 3.4.
- Director 1 oder höher
- Datenbank: Es erfolgen ein Upgrade des Schemas und eine Migration der Daten der Sitedatenbank (sowie der Konfigurationsprotokollierungsdatenbank und der Überwachungsdatenbank, sofern eine frühere 7.x-Version aktualisiert wird).
- Personal vDisk

Aktualisieren Sie, falls erforderlich, anhand der Informationen in der Feature-/Produktdokumentation die folgenden Elemente:

- Provisioning Services (für XenApp 7.x und XenDesktop 7.x empfiehlt Citrix, dass Sie die aktuelle freigegebene Version verwenden; die unterstützte Mindestversion ist Provisioning Services 7.0).
  - Aktualisieren Sie den Provisioning Services-Server mit dem parallelen Serverupgrade und die Clients mit der vDisk-Versionsverwaltung.
  - Provisioning Services 7.x unterstützt nicht das Erstellen von neuen Desktops mit Versionen von XenDesktop 5. Obwohl vorhandene Desktops weiterhin funktionieren, können Sie daher mit Provisioning Services 7.x erst dann neue Desktops erstellen, wenn Sie für XenDesktop ein Upgrade durchgeführt haben. Wenn Sie eine heterogene Umgebung mit XenDesktop 5.6 und XenDesktop 7.x-Sites planen, führen Sie daher kein Upgrade von Provisioning Services auf Version 7 durch.
- Microsoft System Center Virtual Machine Manager SCVMM. Das aktuelle Produkt unterstützt SCVMM 2012 und SCVMM 2012 SP1. XenDesktop 5.x unterstützt frühere Versionen. Verwenden Sie zur Minimierung von Ausfallzeiten die folgende Upgradereihenfolge:
  1. Wenn Sie Controller mit Versionen vor XenDesktop 5.6 FP1 haben, aktualisieren Sie diese auf XenDesktop 5.6 FP1 (siehe XenDesktop-Dokumentation für Version 5.6 FP1).
  2. Aktualisieren Sie die SCVMM-Server auf SCVMM 2012 (Anweisungen finden Sie in der Dokumentation von Microsoft).
  3. Aktualisieren Sie die XenDesktop-Komponenten auf die aktuelle Version.
  4. Falls gewünscht, können Sie ein Upgrade des SCVMM-Servers auf SCVMM 2012 SP1 durchführen.
- StoreFront:

# Anforderungen, Einschränkungen und Vorbereitung

- Sie müssen die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle des Installationsprogramms für das Upgrade der Kernkomponenten und VDAs verwenden. Sie können keine Daten von einer früheren Version importieren oder migrieren.
- Wenn Sie Komponenten auf die neue Version aktualisieren, andere Komponenten (auf anderen Maschinen) jedoch nicht, wird von Studio eine Erinnerung ausgegeben. Beispiel: Wenn ein Upgrade neue Versionen von Controller und Studio enthält und Sie nur den Controller aktualisieren (jedoch das Installationsprogramm auf der Maschine, auf der Studio installiert ist, nicht ausführen) lässt Studio eine Verwaltung der Site erst dann wieder zu, wenn Sie auch für Studio ein Upgrade durchgeführt haben.
- Stellen Sie vor dem Upgrade des Citrix Lizenzservers sicher, dass Ihr Subscription Advantage-Datum für die neue Produktversion gültig ist. Wenn Sie ein Upgrade einer früheren 7.x-Produktversion durchführen, muss das Datum mindestens 2016.0518 sein.
- Sie können kein Upgrade von XenDesktop Express Edition durchführen. Beschaffen und installieren Sie eine Lizenz für eine derzeit unterstützte Edition und führen Sie anschließend ein Upgrade durch.
- Vor Beginn einer Upgradeaktivität sichern Sie die Datenbank (siehe CTX135207), damit Sie sie im Falle eines Problems


© 1999-2017 Citrix Systems, Inc. All rights reserved.

nach dem Datenbankupgrade wieder herstellen können.
- Optional können Sie Vorlagen sichern und evtl. verwendete Hypervisors aktualisieren.
- Stellen Sie vor dem Upgrade sicher, dass die Site stabil und funktionsfähig ist. Bestehen bei einer Site Probleme, werden diese durch ein Upgrade nicht behoben. Stattdessen kann das Upgrade zusätzliche Probleme verursachen, die sich nur schwer beheben lassen.
- Bevor Sie ein Upgrade durchführen, schließen Sie alle Programme, die Dateisperren verursachen könnten, einschließlich Verwaltungskonsolen und PowerShell-Sitzungen. (Das Neustarten der Maschine stellt sicher, dass alle Dateisperren aufgehoben werden und keine Windows-Updates ausstehen.)
- Wenn Sie Sites einer früheren Version neben Sites der aktuellen Version beibehalten müssen, lesen Sie den Abschnitt Hinweise zu heterogenen Umgebungen.
- Wenn Sie VDAs unter Windows XP oder Windows Vista installiert haben, lesen Sie den Abschnitt VDAs auf Maschinen mit Windows XP oder Windows Vista.
- Wenn Sie nicht alle VDAs auf die aktuelle Version aktualisieren möchten, lesen Sie Unterstützung gemischter VDAs.
- Enthält Ihre Bereitstellung Webinterface, empfiehlt Citrix die Verwendung von StoreFront.
- Auf den Maschinen, auf denen Sie die Produktkomponenten aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.
- Lesen Sie den Abschnitt zur Upgradereihenfolge, damit Sie mögliche Ausfälle einplanen und das Risiko entschärfen können.

In folgenden Situationen ist kein Upgrade möglich:

- Bei einer Early Release- oder Technology Preview-Version
- Bei einer XenApp-Version vor 7.5 (außer Sie ersetzen XenApp 6.5-Software auf einem Server mit einem aktuellen VDA für Serverbetriebssysteme, siehe Migrieren von XenApp 6.x)
- Bei einer XenDesktop-Version vor Version 5.6, siehe Migrieren von XenDesktop 4.
- Von XenApp auf XenDesktop oder von XenDesktop auf XenApp

**Empfehlung:** Prüfen Sie vor dem Upgrade und während des Upgrades die Integrität des Systems. Führen Sie **Site testen** zu den folgenden Zeitpunkten aus:

- Bevor Sie Backups erstellen
- Nach jedem Controllerupgrade
- Nach dem Upgrade von VDAs und anderer Komponenten
- Nach dem Upgrade der Site über Studio

# Hinweise zu heterogenen Umgebungen

Wenn Ihre Umgebung Sites/Farmen mit mehreren Produktversionen enthält (heterogene Umgebung), empfiehlt Citrix die Verwendung von StoreFront zum Aggregieren von Anwendungen und Desktops aus den unterschiedlichen Produktversionen (Beispiel: Sie haben eine XenDesktop 7.1-Site und eine XenDesktop 7.5-Site). Weitere Informationen finden Sie in der Dokumentation zu StoreFront.

- Verwenden Sie in einer heterogenen Umgebung weiterhin Studio und Director für das jeweilige Release. Die verschiedenen Versionen müssen jedoch auf separaten Maschinen installiert sein.
- Wenn Sie XenDesktop 5.6 und XenDesktop 7.x-Sites parallel ausführen und für beide Provisioning Services verwenden möchten, stellen Sie entweder eine neue Version von Provisioning Services für die Verwendung mit der 7.x-Site bereit oder aktualisieren Sie die aktuelle Version von Provisioning Services. In diesem Fall können Sie jedoch keine neuen

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Arbeitslasten in der XenDesktop 5.6-Site mehr bereitstellen.

Citrix empfiehlt, in einer Site jeweils alle Komponenten zu aktualisieren. Sie können zwar von einigen Komponenten die früheren Versionen verwenden, jedoch sind u. U: nicht alle Features einer aktuellen Version verfügbar. Beispiel: Sie können zwar aktuelle VDAs in Bereitstellungen mit älteren Controllerversionen verwenden, jedoch sind die neuen Features des aktuellen Releases möglicherweise nicht verfügbar. Bei der Registrierung des VDAs können beim Verwenden nicht aktueller Versionen ebenfalls Probleme auftreten. Weitere Informationen finden Sie unter Hinweise zu gemischten VDAs.

- Sites mit Controllern der Version 5.x und VDAs der Version 7.x sollten in diesem Zustand nur vorübergehend verbleiben. Im Idealfall sollten Sie das Upgrade aller Komponenten so schnell wie möglich durchführen.
- Führen Sie ein Upgrade einer eigenständigen Studio-Version erst dann durch, wenn Sie zur Verwendung der neuen Version bereit sind.

# VDAs auf Maschinen mit Windows XP oder Windows Vista

Sie können kein Upgrade von VDAs auf Maschinen mit Windows XP oder Windows Vista auf eine 7.x-Version durchführen. Sie müssen VDA 5.6 FP1 mit bestimmten Hotfixes verwenden. Anweisungen hierfür finden Sie unter CTX140941. Obwohl ältere VDAs in einer 7.x-Site funktionieren, können zahlreiche Features nicht verwendet werden. Beispiele:

- Features in Studio, die eine neuere VDA-Version erfordern
- Konfiguration von App-V-Anwendungen über Studio
- Konfiguration von Receiver StoreFront-Adressen über Studio
- Automatische Unterstützung der Microsoft Windows-KMS-Lizenzierung bei Verwendung von Maschinenerstellungsdiensten Siehe CTX128580.
- Informationen in Director:
  - Anmeldezeiten und Anmeldeende-Ereignisse, die sich auf die Anmeldungsdauer auswirken, in den Ansichten "Dashboard", "Trends" und "Benutzerdetails"
  - Eine Aufschlüsselung der Anmeldedauer für HDX-Verbindungs- und Authentifizierungszeiten sowie Zeitdauerangaben für Profil- und GPO-Ladevorgänge, Anmeldeskript und die Herstellung interaktiver Sitzungen
  - Einige Kategorien der Fehlerraten für Maschinen und Verbindungen
  - Aktivitätsmanager in der Ansicht "Helpdesk" und "Benutzerdetails"

Citrix empfiehlt ein Reimaging der Windows XP- und Windows Vista-Maschinen unter einer unterstützten Betriebssystemversion und die anschließende Installation der aktuellen VDA-Version.

# VDAs auf Maschinen mit Windows 8.x oder Windows 7

Für ein Upgrade von VDAs auf Maschinen mit Windows 8.x oder Windows 7 auf Windows 10 empfiehlt Citrix ein Reimaging der Maschinen mit Windows 7 und 8.x auf Windows 10 und die anschließende Installation der VDAs für Windows 10. Ist ein Reimaging nicht möglich, deinstallieren Sie den VDA vor dem Upgrade des Betriebssystems, da er ansonsten einen nicht unterstützten Zustand annimmt.

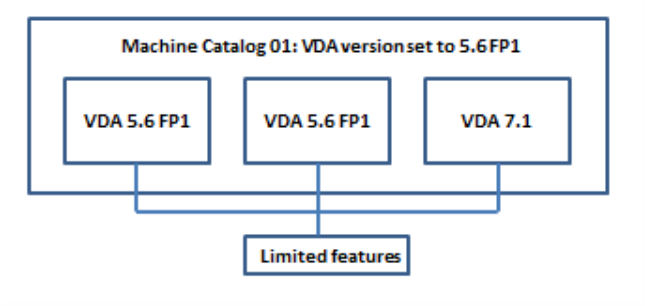

© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Unterstützung gemischter VDAs

Für ein Upgrade des Produkts auf eine neuere Version empfiehlt Citrix, dass Sie alle Kernkomponenten und VDAs aktualisieren, damit Sie alle neuen und verbesserten Features der Edition verwenden können. Beispiel: Zur Verwendung der Features Sitzungsvorabstart, Sitzungsfortbestehen und nicht authentifizierte Benutzer des Releases 7.6 müssen die VDAs mindestens in Version 7.6 vorliegen.

In einigen Umgebungen ist ein Upgrade aller VDAs auf die aktuelle Version möglicherweise nicht möglich. In diesem Fall können Sie beim Erstellen eines Maschinenkatalogs die auf den Maschinen installierte VDA-Version angeben. Standardmäßig ist für diese Einstellung die neueste empfohlene VDA-Version festgelegt. Sie müssen eine Änderung dieser Einstellung nur dann in Betracht ziehen, wenn der Maschinenkatalog Maschinen mit früheren VDA-Versionen enthält. Das Vorhandensein mehrerer VDA-Versionen im selben Maschinenkatalog kann jedoch unerwünschte Auswirkungen haben.

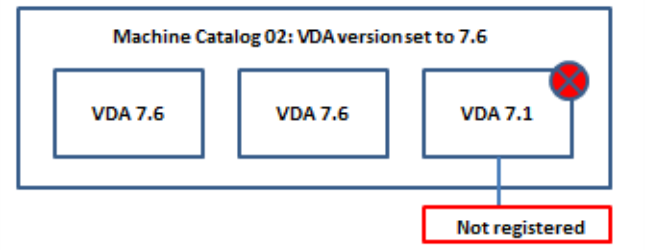
Wie oben erwähnt muss in Bereitstellungen mit Windows XP- und Windows Vista-Systemen eine frühere VDA-Version verwendet werden. Für den Maschinenkatalog, der die entsprechenden Maschinen enthält, muss VDA Version 5.6 FP1 festgelegt werden. Die VDAs können sich erfolgreich beim Controller registrieren, doch die Maschinen können viele der neuen Features der 7.x-Versionen (einschließlich StoreFront) nicht verwenden. Das Gleiche gilt für Maschinen mit VDAs der Version 7.x, die Sie einem solchen Katalog hinzufügen. Dies wird in der folgenden Abbildung dargestellt.




Wenn Sie wie im o. g. Fall ältere VDAs weiterhin verwenden müssen, fassen Sie diese in einem eigenen Maschinenkatalog zusammen.

Wenn ein Maschinenkatalog mit der standardmäßig empfohlenen VDA-Versionseinstellung erstellt wird und auf Maschinen in dem Katalog eine frühere VDA-Version installiert ist, können sich diese Maschinen nicht beim Controller registrieren und funktionieren nicht.

Beispiel (aktuelle VDA-Version sei 7.6): Sie erstellen einen Maschinenkatalog mit der VDA-Standardeinstellung: "7.6 (für die neuesten Features empfohlen)". Sie fügen dem Katalog drei Maschinen hinzu, zwei mit VDA 7.6 und eine mit VDA 7.1.



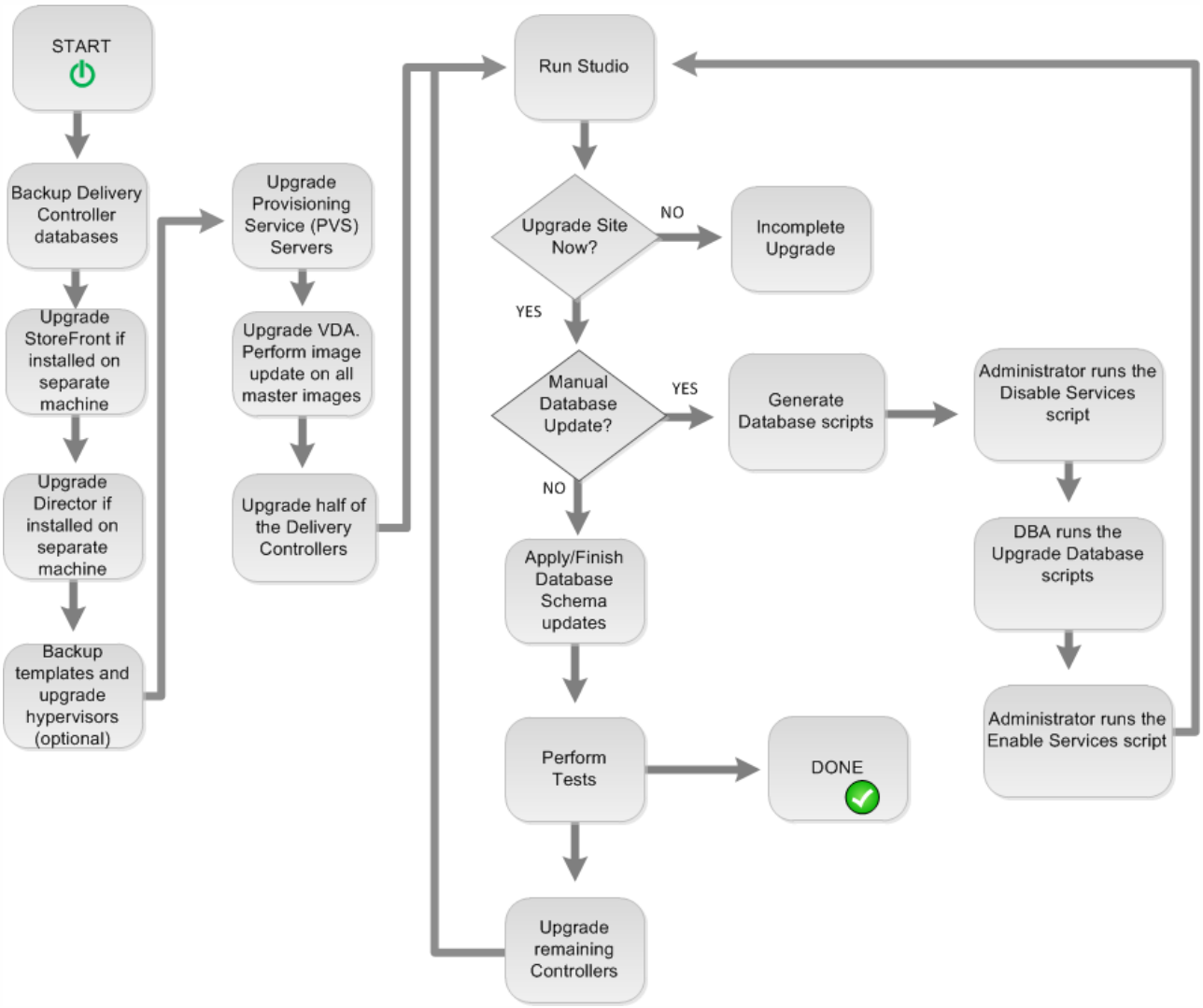

Die Maschine mit VDA 7.1 kann sich in diesem Fall nicht beim Controller registrieren. Wenn Sie kein Upgrade dieses VDAs durchführen können, können Sie einen separaten Maschinenkatalog mit einer VDA-Einstellung von Version 7.0 oder höher


© 1999-2017 Citrix Systems, Inc. All rights reserved.

erstellen und diesem die Maschine hinzufügen. Die Maschine kann dann zwar die neuen Features der Version 7.6 nicht nutzen, sie kann sich jedoch beim Controller registrieren.

# Aktualisierungsreihenfolge

Die Upgradereihenfolge ist unten dargestellt, Erläuterungen folgen. Werden Komponenten auf verschiedenen Maschinen installiert, führen Sie das Installationsprogramm auf jeder Maschine aus.




## Aktualisieren von Komponenten

Zum Ausführen der grafischen Oberfläche des Installationsprogramms melden Sie sich bei der Maschine an und legen Sie anschließend das Installationsmedium ein oder stellen Sie das ISO-Laufwerk für das neue Release bereit. Doppelklicken Sie auf **Automatische Auswahl**. Anweisungen zur Verwendung der Befehlszeilenschnittstelle finden Sie unter "Installieren über die Befehlszeile".

1. Wenn mehrere Kernkomponenten (z. B. Controller, Studio und Lizenzserver) auf dem gleichen Server installiert sind und für mehrere dieser Komponenten eine neue Version verfügbar ist, werden alle beim Ausführen des Installationsprogramms


© 1999-2017 Citrix Systems, Inc. All rights reserved.

auf dem Server aktualisiert. Wenn Kernkomponenten auf anderen Maschinen als dem Controller installiert sind, führen Sie das Installationsprogramm auf diesen Maschinen aus (empfohlene Reihenfolge: Lizenzserver, StoreFront und dann Director).

2. Aktualisieren Sie die Provisioning Services-Server und -Clients (Anweisungen hierzu finden Sie in der Dokumentation zu Provisioning Services).
3. Führen Sie das Produktinstallationsprogramm auf Maschinen mit VDAs aus. Sie können zwar ein Upgrade der VDAs vor oder nach dem Upgrade des Controllers durchführen, Citrix empfiehlt jedoch ein Upgrade vor dem des Controllers, damit anschließend neue Features schnell aktiviert werden können.
   Wenn Sie ein Upgrade für VDAs von einer früheren 7.x-Version auf physischen Maschinen (einschließlich Remote-PC-Zugriff-Maschinen) durchführen, verwenden Sie die Befehlszeilenschnittstelle mit dem folgenden Parameter: /EXCLUDE "Personal vDisk","Machine Identity Service". Beispiel:

   C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"

4. Führen Sie das Produktinstallationsprogramm auf der Hälfte der Controller aus. (Damit werden auch alle anderen Kernkomponenten auf diesen Servern aktualisiert.) Wenn Ihre Site beispielsweise vier Controller enthält, führen Sie das Installationsprogramm auf zwei Controllern aus.
   - Dadurch dass die Hälfte der Controller aktiv bleibt, können Benutzer auf die Site zugreifen. Die VDAs können sich bei den anderen Controllern registrieren. Zeitweise wird die Site möglicherweise mit reduzierter Kapazität ausgeführt, da weniger Controller verfügbar sind. Durch das Upgrade wird nur für das Einrichten neuer Clientverbindungen während der letzten Datenbankaktualisierungsschritte eine kurze Unterbrechung verursacht. Die aktualisierten Controller können Anforderungen erst verarbeiten, wenn die gesamte Site aktualisiert wurde.
   - Wenn die Site nur einen Controller hat, ist sie während des Upgrades nicht funktionsfähig.
5. Ist Studio auf einer anderen Maschine installiert als einer der im vorherigen Schritt aktualisierten Controller, führen Sie das Installationsprogramm auf der Maschine aus, auf der Studio installiert ist.
6. Führen Sie über die neu aktualisierte Studio-Version ein Upgrade der Sitedatenbank aus. Einzelheiten finden Sie unter Aktualisieren der Datenbank und Site.
7. Wählen Sie in der neu aktualisierten Studio-Version im Navigationsbereich **Citrix Studio** *Sitename* aus. Wählen Sie die Registerkarte **Häufige Aufgaben**. Wählen Sie **Upgrade der übrigen Delivery Controller durchführen**.
8. Nach Abschluss des Upgrades und Bestätigen von dessen Durchführung schließen Sie Studio und öffnen Sie es erneut.
9. Wählen Sie auf der Seite "Häufige Aufgaben" im Abschnitt "Sitekonfiguration" die Option **Registrierung durchführen**. Durch das Registrieren der Controller werden diese für die Site verfügbar.
10. Nach Auswahl von **Fertig stellen** im Anschluss an das Upgrade können Sie sich optional für die Teilnahme beim Programm zur Verbesserung der Benutzerfreundlichkeit von Citrix (Customer Experience Improvement Program, CEIP) registrieren, durch das anonyme Informationen zu Ihrer Bereitstellung gesammelt werden. Diese Informationen werden Verbesserung von Qualität, Zuverlässigkeit und Leistung des Produkts verwendet.
11. Nach dem Upgrade von Komponenten, Datenbank und Site führen Sie mit Studio folgende Arbeitsgänge durch:
    - Testen Sie die neu aktualisierte Site. Wählen Sie in Studio im Navigationsbereich **Citrix Studio** *Sitename*. Wählen Sie die Registerkarte **Häufige Aufgaben** und dann **Site testen**. Diese Tests werden automatisch nach dem Upgrade der Datenbank ausgeführt, Sie können sie jedoch jederzeit wiederholen.
    - Aktualisieren Sie alle Masterimages, die den aktualisierten VDA verwenden.
    - Aktualisieren Sie Maschinenkataloge und Bereitstellungsgruppen.

### Aktualisieren von Sitedatenbank und Site

Nach dem Upgrade der Kernkomponenten und VDAs verwenden Sie die neu aktualisierte Studio-Version für ein automatisches oder manuelles Upgrade von Datenbank und Site.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Für ein automatisches Datenbankupgrade müssen die Berechtigungen des Studio-Benutzers die Berechtigung zum Aktualisieren des SQL Server-Datenbankschemas umfassen (z. B. Datenbankrolle "db_securityadmin" oder "db_owner"). Weitere Informationen finden Sie im Artikel "Datenbanken".
- Hat der Benutzer diese Berechtigungen nicht, werden bei einem manuellen Datenbankupgrade Skripts generiert. Der Studio-Benutzer führt einige dieser Skripts über Studio aus, andere werden vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio ausgeführt. Bei der manuellen Ausführung von SQL-Skripts sollten sie mit dem SQLCMD-Hilfsprogramm oder mit SQL Management Studio im SQLCMD-Modus ausgeführt werden. Andernfalls können Fehler aufgrund von Ungenauigkeiten auftreten.

**Wichtig:** Citrix empfiehlt dringend, die Datenbank vor dem Upgrade zu sichern (siehe CTX135207).
Während des Datenbankupgrades sind die Produktdienste deaktiviert. Während dieser Zeit können Controller keine neuen Verbindungen für die Site verhandeln. Planen Sie daher sorgfältig.

Nach dem Upgrade der Datenbank und der Aktivierung der Produktdienste testet Studio Umgebung und Konfiguration und generiert einen HTML-Bericht. Wenn Probleme identifiziert werden, können Sie die Datenbank aus dem Backup wiederherstellen. Wenn die Probleme beseitigt sind, können Sie die Datenbank erneut aktualisieren.

**Automatisches Upgrade von Datenbank und Site:** Starten Sie die aktualisierte Studio-Version. Sobald Sie das automatische Upgrade der Site gestartet und bestätigt haben, dass Sie bereit sind, beginnt das Upgrade von Datenbank und Site.

**Manuelles Upgrade von Datenbank und Site:** Bei diesem Vorgang werden Skripts generiert.

1. Starten Sie die aktualisierte Studio-Version. Sobald Sie das manuelle Upgrade der Site ausgewählt haben, prüft der Assistent die Kompatibilität des Lizenzservers und fordert eine Bestätigung an. Wenn Sie bestätigt haben, dass Sie die Datenbank gesichert haben, erstellt der Assistent Skripts und eine Checkliste der Upgradeschritte und zeigt diese an.
2. Führen Sie die folgenden Skripts in der angegebenen Reihenfolge aus:

| Skript | Beschreibung |
|---|---|
| DisableServices.ps1 | PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste deaktiviert |
| UpgradeSiteDatabase.sql | SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Sitedatenbank ausgeführt werden muss |
| UpgradeMonitorDatabase.sql | SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Überwachungsdatenbank ausgeführt werden muss |
| UpgradeLoggingDatabase.sql | SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Konfigurationsprotokollierungsdatenbank ausgeführt werden muss Führen Sie dieses Skript nur aus, wenn diese Datenbank geändert wird (z. B. nach dem Anwenden eines Hotfixes). |
| EnableServices.ps1 | PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste aktiviert |

3. Wenn Sie alle angezeigten Checklistenaufgaben erledigt haben, wählen Sie **Upgrade abschließen und zu 'Häufige**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Aufgaben' zurückkehren**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

Jul 08, 2016

Wenn Sie das Installationsprogramm des aktuellen Produkts auf einem XenApp 6.5-Workerserver ausführen, werden folgende Aktionen durchgeführt:

- Der Server wird aus der XenApp 6.5-Farm entfernt (für diese Aufgabe wird automatisch die Befehlszeile des XenApp 6.5-Installationsprogramms aufgerufen)
- Die XenApp 6.5-Software wird entfernt
- Ein neuer (XenApp 7.6 oder ein höheres unterstütztes Release) VDA für Windows-Serverbetriebssysteme wird installiert

Wenn Sie die grafische Benutzeroberfläche des Installationsprogramms verwenden, werden Sie durch denselben Assistenten geführt wie bei der Installation von VDAs für Windows-Serverbetriebssysteme in der neuen XenApp-Site. Auch die Befehlszeile verwendet die gleichen Befehle und Parameter, die Sie für die Installation anderer VDAs verwenden.

**Hinweis:** Sie können zwar einen XenApp 6.5-Workerserver aktualisieren, die Installation des aktuellen VDAs auf einer "sauberen" Maschine bietet jedoch mehr Sicherheit.

Durch die Installation der XenApp-Kernkomponenten und der anderen VDAs sind Sie wahrscheinlich bereits mit dem Installationsprogramm vertraut. Starten Sie das Installationsprogramm (Installieren über die grafische Oberfläche) oder führen Sie den Befehl auf dem XenApp 6.5-Workerserver aus (Installieren über die Befehlszeile).

Gut zu wissen:

- Diese Upgrade ist auf XenApp 6.5-Servern gültig, die im Servermodus "nur Sitzungsmodus" konfiguriert wurden (auch Nur-Sitzungsserver oder Workerserver genannt).
- Das Deinstallieren von XenApp 6.5 erfordert mehrere Serverneustarts. Wenn Sie die Befehlszeile verwenden, können Sie mit der Option /NOREBOOT diese automatische Aktion unterdrücken. Sie müssen den Server jedoch neu starten, damit die Deinstallation und die nachfolgende Neuinstallation ausgeführt werden können.
- Wenn während der XenApp-Deinstallation ein Fehler auftritt, prüfen Sie das in der Fehlermeldung angegebene Deinstallationsfehlerprotokoll. Deinstallationsprotokolldateien befinden sich im Ordner "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\".
- Nach dem Upgrade überprüfen Sie IMA- und HDX-spezifische Systemeinstellungen und Registrierungseinträge. Einige Einstellungen gelten ggf. nicht mehr oder funktionieren anders.
- Nach dem Upgrade der XenApp 6.5-Workerserver erstellen Sie mit Studio in der neuen XenApp-Site Maschinenkataloge (oder bearbeiten Sie vorhandene Kataloge) für die aktualisierten Worker.
- Wenn Sie Richtlinien- und Anwendungseinstellungen von einem XenApp 6.5-Controllerserver migriert haben (siehe Migrieren von XenApp 6.x), weisen Sie die Bereitstellungsgruppen mit den migrierten veröffentlichten Anwendungen dem Maschinenkatalog zu, in dem diese Anwendungen in XenApp 6.5 gehostet wurden.

## Problembehandlung

Symptome: Fehler beim Entfernen der XenApp 6.5-Software. Das Deinstallationsprotokoll enthält die Meldung:"Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

- Ursache: Das Problem tritt auf Systemen auf, wenn (1) Sie während der XenApp 6.5-Erstinstallation angegeben haben, dass der Citrix XML-Dienst (CtxHttp.exe) keinen Port gemeinsam mit IIS verwenden soll, und (2) .NET Framework 3.5.1 installiert ist.
- Lösung:
  1. Entfernen Sie die Webserver (IIS)-Rolle mit dem Windows-Assistenten zum Entfernen von Rollen. (Sie können die Webserver (IIS)-Rolle später wieder installieren.)
  2. Starten Sie den Server neu.
  3. Deinstallieren Sie Folgendes mit der Windows-Funktion zum Installieren und Deinstallieren:
     1. Citrix XenApp 6.5
     2. Microsoft Visual C++ 2005 Redistributable (x64), Version 8.0.56336
  4. Starten Sie den Server neu.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Installieren Sie den VDA für Windows-Serverbetriebssysteme mit dem XenApp-Installationsprogramm.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Migrieren von XenApp 6.x

Jul 08, 2016

Wichtig: Lesen Sie den gesamten Artikel, bevor Sie mit der Migration beginnen.

Das Tool für die Migration von XenApp 6.x (das Migrationstool) ist eine Sammlung von PowerShell-Skripts und Cmdlets, die Richtliniendaten und Farmdaten für XenApp 6.x (6.0 und 6.5) migrieren. Dazu führen Sie auf dem XenApp 6.x-Controllerserver Export-Cmdlets aus, die die Daten in XML-Dateien zusammenfassen. Anschließend führen Sie vom XenApp 7.6-Controller aus die Import-Cmdlets aus, die mit den beim Export gesammelten Daten Objekte erstellen.

Eine Videoübersicht über das Migrationstool ist hier verfügbar.

Unten ist die Abfolge des Migrationsvorgangs zusammengefasst. Details werden später erläutert.

1. Auf einem XenApp 6.0- oder 6.5-Controller:
   1. Importieren Sie die PowerShell-Exportmodule.
   2. Exportieren Sie mit den Export-Cmdlets die Richtlinien- und/oder Farmdaten in XML-Dateien.
2. Kopieren Sie die XML-Dateien (und den Ordner mit den Symbolen, wenn sie für den Export nicht in die XML-Dateien eingebettet werden) auf den XenApp 7.6-Controller.
3. Auf dem XenApp 7.6-Controller:
   1. Importieren Sie die PowerShell-Importmodule.
   2. Importieren Sie mit den Import-Cmdlets die Richtlinien- und/oder Farmdaten (Anwendungen), wobei Sie die XML-Dateien als Eingabe verwenden.
4. Führen Sie die nach der Migration erforderlichen Schritte aus.

Vor der eigentlichen Migration können Sie die XenApp 6.x-Einstellungen exportieren und eine Exportvorschau in der XenApp 7.6-Site ausführen. Die Vorschau lässt mögliche Schwachstellen erkennen, damit Sie die Probleme vor der eigentlichen Migration beheben können. Bei einer Vorschau kann sich beispielsweise herausstellen, dass eine Anwendung mit dem gleichen Namen bereits in der neuen XenApp 7.6-Site vorhanden ist. Sie können die bei der Vorschau erstellten Protokolldateien bei der Migration als Leitfaden verwenden.

Sofern nicht anders angegeben, bezieht sich der Begriff 6.x auf XenApp 6.0 oder 6.5.

## Neue Features in diesem Release

Dieses Dezember 2014-Release (Version 20141125) enthält die folgenden Updates:

- Wenn bei der Verwendung des Migrationstools für eine XenApp 6.x-Farm Probleme auftreten, veröffentlichen Sie einen Bericht im Supportforum http://discussions.citrix.com/forum/1411-xenapp-7x/, sodass Citrix eine Untersuchung durchführen und das Tool verbessern kann.
- Neues Paketformat: Die Datei XAMigration.zip enthält jetzt zwei separate Pakete: ReadIMA.zip und ImportFMA.zip. Zum Exportieren von einem XenApp 6.x-Server benötigen Sie nur die ReadIMA.zip. Zum Importieren auf einen XenApp 7.6.x-Server benötigen Sie nur die ImportFMA.zip.
- Das Cmdlet "Export-XAFarm" unterstützt einen neuen Parameter (EmbedIconData), durch den das Kopieren der Symboldaten in verschiedene Dateien nicht mehr nötig ist.
- Das Cmdlet "Import-XAFarm" unterstützt drei neue Parameter:
  - MatchServer: Zum Importieren von Anwendungen von Servern, deren Namen mit einem Ausdruck übereinstimmen
  - NotMatchServer: Zum Importieren von Anwendungen von Servern, deren Namen nicht mit einem Ausdruck übereinstimmen
  - IncludeDisabledApps: Zum Importieren von deaktivierten Anwendungen
- Vorab gestartete Anwendungen werden nicht importiert.
- Das Cmdlet "Export-Policy" ist für XenDesktop 7.x.

## Migrationstoolpaket

Das Migrationstool ist auf der Citrix Downloadsite unter XenApp 7.6 verfügbar. Die Datei XAMigration.zip enthält zwei separate, unabhängige Pakete:

- ReadIMA.zip: enthält die Dateien zum Exportieren von Daten aus der XenApp 6.x-Farm sowie freigegebene Module.

| Modul bzw. Datei | Beschreibung |
|---|---|
| ExportPolicy.psm1 | PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Richtlinien in eine XML-Datei. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Modul bzw. Datei | Beschreibung |
|---|---|
| ExportXAFarm.psm1 | PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Farmeinstellungen in eine XML-Datei. |
| ExportPolicy.psd1 | PowerShell-Manifestdatei für Skriptmodul ExportPolicy.psm1 |
| ExportXAFarm.psd1 | PowerShell-Manifestdatei für Skriptmodul ExportXAFarm.psm1 |
| LogUtilities.psm1 | Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen |
| XmlUtilities.psd1 | PowerShell-Manifestdatei für Skriptmodul XmlUtilities.psm1 |
| XmlUtilities.psm1 | Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen |

- ImportFMA.zip: enthält die Dateien zum Importieren von Daten aus der XenApp 7.6-Farm sowie freigegebene Module.

| Modul bzw. Datei | Beschreibung |
|---|---|
| ImportPolicy.psm1 | PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6. |
| ImportXAFarm.psm1 | PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6. |
| ImportPolicy.psd1 | PowerShell-Manifestdatei für Skriptmodul ImportPolicy.psm1 |
| ImportXAFarm.psd1 | PowerShell-Manifestdatei für Skriptmodul ImportXAFarm.psm1 |
| PolicyData.xsd | XML-Schema für Richtliniendaten. |
| XAFarmData.xsd | XML-Schema für XenApp-Farmdaten. |
| LogUtilities.psm1 | Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen |
| XmlUtilities.psd1 | PowerShell-Manifestdatei für Skriptmodul XmlUtilities.psm1 |
| XmlUtilities.psm1 | Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen |

### Einschränkungen

- Nicht alle Richtlinieneinstellungen werden importiert; siehe Nicht importierte Richtlinieneinstellungen. Einstellungen, die nicht unterstützt werden, werden ignoriert und in der Protokolldatei angegeben.
- Zwar werden alle Anwendungsdetails während des Exportvorgangs in der XML-Ausgabedatei gesammelt, aber nur auf Servern installierte Anwendungen werden in die XenApp 7.6-Site importiert. Veröffentlichte Desktops, Inhalte und die meisten gestreamten Anwendungen werden nicht unterstützt (Informationen zu Ausnahmen finden Sie unter Schrittweise Anleitungen: Importieren von Daten) im Abschnitt zu den Import-XAFarm-Cmdlet-Parametern.
- Anwendungsserver werden nicht importiert.
- Viele Anwendungseigenschaften werden nicht importiert wegen der Unterschiede zwischen der XenApp 6.x Independent Management Architecture (IMA) und der XenApp 7.6 FlexCast Management Architecture (FMA). Weitere Informationen hierzu finden Sie unter Zuordnung von Anwendungseigenschaften.
- Während des Imports wird eine Bereitstellungsgruppe erstellt. Weitere Informationen zum Filtern des importierten Inhalts mit Parametern finden Sie unter Erweiterte Verwendung.
- Nur Citrix Richtlinieneinstellungen, die mit der AppCenter-Verwaltungskonsole erstellt wurden, werden importiert. Citrix Richtlinieneinstellungen, die mit Windows Gruppenrichtlinienobjekten erstellt wurden, werden nicht importiert.
- Die Migrationsskripts sind nur für die Migrationen von XenApp 6.x auf XenApp 7.6 vorgesehen.
- Mehr als fünffach verschachtelte Ordner werden von Studio nicht unterstützt und werden nicht importiert. Wenn die Ordnerstruktur Ihrer Anwendung Ordner mit mehr als fünf Ebenen von Unterordnern enthält, reduzieren Sie vor dem Importieren die Anzahl der verschachtelten Ordnerebenen.

### Sicherheitsüberlegungen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die durch die Exportskripts erstellten XML-Dateien können vertrauliche Informationen über Ihre Umgebung und Organisation enthalten, z. B. Benutzernamen, Servernamen und andere XenApp-Farm-, Anwendungs- und Richtlinienkonfigurationsdaten. Speichern und verwenden Sie diese Dateien in einer sicheren Umgebung.

Prüfen Sie die XML-Dateien sorgfältig, bevor Sie sie als Eingabe für den Import von Richtlinien und Anwendungen verwenden, um sicherzustellen, dass sie keine unbefugten Änderungen enthalten.

Richtlinienobjektzuweisungen (bisher "Richtlinienfilter") steuern die Anwendung von Richtlinien. Nach dem Importieren von Richtlinien prüfen Sie die Objektzuweisungen für jede Richtlinie sorgfältig, um sicherzustellen, dass durch den Import keine Sicherheitsrisiken entstanden sind. Nach dem Import können auf die Richtlinie verschiedene Gruppen von Benutzern, IP-Adressen oder Clientnamen angewendet werden. Die Einstellungen zum Zulassen und Verweigern haben möglicherweise nach dem Import eine andere Bedeutung.

### Protokollierung und Fehlerbehandlung

Die Skripts sorgen für umfangreiche Protokollierung, wobei die Ausführung aller Cmdlets, informative Meldungen, die Ergebnisse der Cmdlet-Ausführung sowie Warnungen und Fehler aufgezeichnet werden.

- Die Verwendung der Citrix PowerShell-Cmdlets wird größtenteils protokolliert. Alle PowerShell-Cmdlets in den Importskripts, die neue Siteobjekte erstellen, werden protokolliert.
- Der Skriptausführungsverlauf wird protokolliert, einschließlich der Objekte, die verarbeitet werden.
- Große Aktionen, die sich auf den Flussstatus auswirken, werden protokolliert, einschließlich über die Befehlszeile geleitete Flüsse.
- Alle Meldungen, die auf der Konsole gedruckt werden, einschließlich Warnungen und Fehler werden protokolliert.
- Jede Zeile wird mit einem Zeitstempel versehen, der auf die Millisekunde genau ist.

Citrix empfiehlt, dass Sie beim Ausführen der Export- und Import-Cmdlets jeweils eine Protokolldatei angeben.

Wenn Sie keinen Protokolldateinamen angeben, wird die Protokolldatei im Basisordner des aktuellen Benutzers (in der PowerShell-Variable $HOME angegeben) gespeichert. Wenn dieser Ordner nicht vorhanden ist, wird die Protokolldatei im aktuellen Ausführungsordner des Skripts gespeichert. Der Standardname der Protokolldatei ist "XFarmYYYYMMDDHHmmSS-xxxxxx", wobei die letzten sechs Ziffern eine zufällige Zahl sind.

Standardmäßig werden die gesamten Fortschrittsinformationen angezeigt. Um die Anzeige zu unterdrücken, legen Sie den NoDetails-Parameter in den Export- und Import-Cmdlets fest.

Bei einem Fehler wird die Ausführung eines Skripts im Allgemeinen angehalten. Wenn der Fehler behoben ist, können Sie das Cmdlet noch einmal ausführen.

Bedingungen, die nicht als Fehler gelten, werden protokolliert und oft als Warnung gemeldet, während die Skriptausführung fortgesetzt wird. Beispielsweise werden nicht unterstützte Anwendungstypen als Warnung gemeldet und nicht importiert. Anwendungen, die bereits in der XenApp 7.6-Site vorhanden sind, werden nicht importiert. Richtlinieneinstellungen, die in XenApp 7.6 veraltet sind, werden nicht importiert.

Die Migrationsskripts verwenden viele PowerShell-Cmdlets und nicht alle möglichen Fehler werden protokolliert. Zusätzliche Protokollierungsfunktionen sind mit den PowerShell-Protokollierungsfeatures verfügbar. Beispielsweise wird alles, was auf dem Bildschirm gedruckt wird, in PowerShell-Aufzeichnungen protokolliert. Weitere Informationen finden Sie in der Hilfe zu den Cmdlets "Start-Transcript" und "Stop-Transcript".

### Anforderungen, Vorbereitungen und Best Practices

Wichtig: Lesen Sie den gesamten Artikel, bevor Sie mit der Migration beginnen.
Sie sollten die grundlegenden PowerShell-Konzepte der Ausführungsrichtlinie, Module, Cmdlets und Skripts verstehen. Obwohl umfangreiche Erfahrung in der Erstellung von Skripts nicht erforderlich ist, sollten Sie die ausgeführten Cmdlets verstehen. Mit dem Cmdlet "Get-Help" können Sie sich die Hilfe zu jedem Migrations-Cmdlet ansehen, bevor Sie es ausführen. Beispiel:

```
Get-Help -full Import-XAFarm
```

Geben Sie eine Protokolldatei in der Befehlszeile an und überprüfen Sie die Protokolldatei jedes Mal, nachdem Sie ein Cmdlet ausgeführt haben. Wenn ein Skript fehlschlägt, identifizieren Sie den Fehler mit der Protokolldatei und beheben Sie ihn. Führen Sie dann das Cmdlet noch einmal aus.

**Gut zu wissen**:

- Zur Vereinfachung der Bereitstellung von Anwendungen während der Ausführung beider Bereitstellungen (vorhandene XenApp 6.x-Farm und neue XenApp 7.6-Site) können Sie beide Bereitstellungen in StoreFront oder dem Webinterface aggregieren. Weitere Informationen zu Ihrem StoreFront- oder Webinterface-Release finden Sie in der Dokumentation in den eDocs (Verwalten > Store erstellen).
- Für die Handhabung der Anwendungssymboldaten gibt es zwei Möglichkeiten:
  - Wenn Sie den Parameter "EmbedIconData" im Cmdlet "Export-XAFarm" angeben, werden exportierte Anwendungssymboldaten in der XML-Ausgabedatei eingebettet.
  - Wenn Sie den Parameter "EmbedIconData" im Cmdlet "Export-XAFarm" nicht angeben, werden exportierte Anwendungssymboldaten werden in einem Ordner gespeichert. Der Name des Ordners wird durch Anfügen der Zeichenfolge "-icons" an den Basisnamen der XML-Ausgabedatei erstellt. Wenn der Parameter "XmlOutputFile" beispielsweise "FarmData.xml" ist, wird der Ordner "FarmData-icons" zum Speichern der Anwendungssymbole erstellt.
    Die Symboldatendateien in diesem Ordner sind TXT-Dateien, die nach den Browsernamen der veröffentlichten Anwendungen benannt sind (die Dateien sind zwar TXT-Dateien, die gespeicherten Daten sind jedoch verschlüsselte binäre Symboldaten, die vom Importskript zum erneuten Erstellen des Anwendungssymbols gelesen werden können). Wenn der Symbolordner während des Importvorgangs nicht im selben Verzeichnis gefunden wird wie die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

XML-Importdatei, werden allgemeine Symbole für die importierten Anwendungen verwendet.

- Die Namen der Skriptmodule, Manifestdateien, freigegebenen Module und Cmdlets sind ähnlich. Verwenden Sie die Tabulatortaste vorsichtig, damit es nicht zu Fehlern kommt. Beispiel: Export-XAFarm ist ein Cmdlet. ExportXAFarm.psd1 und ExportXAFarm.psm1 sind Dateien, die nicht ausgeführt werden können.
- In den nachfolgenden schrittweisen Anleitungen sind die meisten Parameterwerte für <string> mit Anführungszeichen versehen. Diese sind optional für Zeichenfolgen, die nur aus einem Wort bestehen.

**Für den Export des XenApp 6.x-Servers gilt Folgendes**:
- Der Export muss auf einem XenApp 6.x-Server ausgeführt werden, der mit dem Servermodus Controller- und Sitzungshostmodus (üblicherweise Controller genannt) konfiguriert wurde.
- Zum Ausführen der Export-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen von Objekten sein. Sie müssen auch über die erforderlichen Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- Stellen Sie sicher, dass die XenApp 6.x-Farm funktionsfähig ist, bevor Sie mit dem Export beginnen. Sichern Sie die Farmdatenbank. Überprüfen Sie die Integrität der Farm mit dem Dienstprogramm "Citrix IMA Helper" (CTX133983): Führen Sie von der Registerkarte für den IMA Datastore aus einen Master Check aus (und lösen Sie alle ungültigen Einträge mit der Option "DSCheck" auf). Durch das Reparieren von Problemen vor der Migration werden Fehler beim Export vermieden. Wenn ein Server beispielsweise nicht richtig aus der Farm entfernt wird, bleiben seine Daten möglicherweise in der Datenbank vorhanden, was zu Fehlern bei den Cmdlets im Exportskript führen kann (z. B. Get-XAServer -ZoneName). Wenn die Cmdlets fehlschlagen, schlägt das Skript fehl.
- Sie können die Export-Cmdlets auf einer funktionierenden Farm ausführen, die aktive Benutzerverbindungen hat. Die Exportskripts lesen nur die statische Farmkonfiguration und die Richtliniendaten.

**Für den Import auf den XenApp 7.6-Server gilt Folgendes**:
- Sie können Daten in XenApp 7.6-Bereitstellungen (und höhere unterstützte Versionen) importieren. Sie müssen einen XenApp 7.6-Controller und Studio installieren und eine Site erstellen, bevor Sie die aus der XenApp 6.x-Farm exportierten Daten importieren. VDAs sind zwar zum Importieren von Einstellungen nicht erforderlich, sie gestatten jedoch das Verfügbarmachen von Anwendungsdateitypen.
- Zum Ausführen der Import-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen und Erstellen von Objekten sein. Ein Volladministrator hat diese Berechtigungen. Sie müssen auch über die erforderlichen Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- Während eines Imports dürfen keine anderen Benutzerverbindungen aktiv sein. Die Importskripts erstellen viele neue Objekte und wenn andere Benutzer gleichzeitig Änderungen an der Konfiguration vornehmen, können Unterbrechungen auftreten.

Sie können Daten exportieren und dann den Parameter "-Preview " für das Import-Cmdlet verwenden, um eine Vorschau des Imports zu sehen, ohne dass tatsächliche Importvorgänge stattfinden. In den Protokollen wird genau angegeben, was während eines tatsächlichen Importvorgangs passieren würde. Wenn Fehler auftreten, können Sie diese beheben, bevor Sie einen tatsächlichen Import durchführen.

### Schrittweise Anleitungen: Exportieren von Daten

Ein Video des Exports ist hier verfügbar.

Führen Sie die folgenden Schritte aus, um Daten aus einem XenApp 6.x-Controller in XML-Dateien zu exportieren.

1. Laden Sie das Paket mit dem Migrationstool (XAMigration.zip) von der Citrix Downloadsite herunter. Speichern Sie es der Einfachheit halber in einer Netzwerkfreigabe, damit von der XenApp 6.x-Farm und der XenApp 7.6-Site darauf zugegriffen werden kann. Entzippen Sie XAMigration.zip in der Netzwerkfreigabe. Sie sollten nun zwei ZIP-Dateien haben: ReadIMA.zip und ImportFMA.zip.
2. Melden Sie sich am XenApp 6.x-Controller als XenApp-Administrator mit mindestens Lesezugriff und Windows-Berechtigung zum Ausführen von PowerShell-Skripts an.
3. Kopieren Sie die Datei ReadIMA.zip von der Netzwerkfreigabe auf den XenApp 6.x-Controller. Entzippen und extrahieren Sie ReadIMA.zip auf dem Controller in einen Ordner (z. B.: C:\XAMigration).
4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest. Beispiel:
   cd C:\XAMigration
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von Get-ExecutionPolicy.
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf "RemoteSigned" fest, damit die Skripts ausgeführt werden können. Beispiel:
   Set-ExecutionPolicy RemoteSigned
7. Importieren Sie die Moduldefinitionsdateien "ExportPolicy.psd1" und "ExportXAFarm.psd1":
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

   **Gut zu wissen**:
   - Wenn Sie nur Richtliniendaten exportieren möchten, können Sie nur die Moduldefinitionsdatei "ExportPolicy.psd1" importieren. Genauso gilt, wenn Sie nur Farmdaten exportieren möchten, importieren Sie nur "ExportXAFarm.psd1".
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung .psm1.
8. Führen Sie zum Exportieren von Richtliniendaten das Cmdlet Export-Policy aus.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Parameter | Beschreibung |
|---|---|
| -XmlOutputFile "<string>.xml" | Name der XML-Ausgabedatei. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein.<br><br>Standardwert: Keiner. Dieser Parameter ist erforderlich. |
| -LogFile " <string>" | Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter "NoClobber" ebenfalls angegeben ist, wird ein Fehler generiert, sonst wird der Inhalt der Datei überschrieben.<br><br>Standardwert: siehe Protokollierung und Fehlerbehandlung |
| -NoLog | Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist.<br><br>Standardwert: False; Protokollausgabe wird erstellt |
| -NoClobber | Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung.<br><br>Standardwert: False; eine vorhandene Protokolldatei wird überschrieben |
| -NoDetails | Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden.<br><br>Standardwert: False; ausführliche Berichte werden an der Konsole gesendet |
| -SuppressLogo | Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen.<br><br>Standardwert: False; die Meldung wird auf der Konsole gedruckt |

Beispiel: Das folgende Cmdlet exportiert Richtlinieninformationen in die XML-Datei "MyPolicies.xml". Der Vorgang wird in der Datei "MyPolicies.log" protokolliert.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Führen Sie zum Exportieren von Farmdaten das Cmdlet Export-XAFarm aus und geben Sie dabei eine Protokolldatei und eine XML-Datei an.

| Parameter | Beschreibung |
|---|---|
| -XmlOutputFile "<string>.xml" | Name der XML-Ausgabedatei. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein.<br><br>Standardwert: Keiner. Dieser Parameter ist erforderlich. |
| -LogFile " <string>" | Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter "NoClobber" ebenfalls angegeben ist, wird ein Fehler generiert, sonst wird der Inhalt der Datei überschrieben.<br><br>Standardwert: siehe Protokollierung und Fehlerbehandlung |
| -NoLog | Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist.<br><br>Standardwert: False; Protokollausgabe wird erstellt |
| -NoClobber | Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung.<br><br>Standardwert: False; eine vorhandene Protokolldatei wird überschrieben |
| -NoDetails | Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Parameter | Beschreibung |
|---|---|
| | Standardwert: False; ausführliche Berichte werden an der Konsole gesendet |
| -SuppressLogo | Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen.<br><br>Standardwert: False; die Meldung wird auf der Konsole gedruckt |
| -IgnoreAdmins | Administratorinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: False; Administratorinformationen werden exportiert |
| -IgnoreApps | Anwendungsinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: False; Anwendungsinformationen werden exportiert |
| -IgnoreServers | Serverinformationen nicht exportieren.<br><br>Standardwert: False; Serverinformationen werden exportiert |
| -IgnoreZones | Zoneninformationen nicht exportieren.<br><br>Standard: False; Zoneninformationen werden exportiert |
| -IgnoreOthers | Daten wie Folgende nicht exportieren: Konfigurationsprotokollierung, Lastauswertungsprogramme, Lastausgleichsrichtlinien, Druckertreiber und Workergruppen.<br><br>Standardwert: False; andere Informationen werden exportiert<br><br>Hinweis: Der Schalter -IgnoreOthers ermöglicht das Durchführen eines Exports, wenn ein Fehler vorliegt, der keine Auswirkungen auf die exportierten oder importierten Daten hat. |
| -AppLimit <integer> | Anzahl der Anwendungen, die exportiert werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Alle Anwendungen werden exportiert |
| -EmbedIconData | Anwendungssymboldaten in die gleiche XML-Datei einbetten wie die anderen Objekte.<br><br>Standard: Symbole werden separat gespeichert. Weitere Informationen finden Sie unter Anforderungen, Vorbereitungen und Best Practices. |
| -SkipApps <integer> | Anzahl der Anwendungen, die übersprungen werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Anwendungen werden übersprungen |

Beispiel: Das folgende Cmdlet exportiert Farminformationen in die XML-Datei "MyFarm.xml". Der Vorgang wird in der Datei "MyFarm.log" protokolliert. Ein Ordner mit dem Namen "MyFarm-icons" wird zum Speichern der Datendateien für die Anwendungssymbole erstellt. Dieser Ordner ist am gleichen Speicherort wie "MyFarm.xml".

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"
```

Nachdem die Ausführung der Exportskripts abgeschlossen ist, enthalten die in den Befehlszeilen angegebenen XML-Dateien die Richtliniendaten und die XenApp-Farmdaten. Die Anwendungssymboldateien enthalten die Symboldatendateien und die Protokolldatei gibt an, was sich beim Export ereignet hat.

### Schrittweise Anleitungen: Importieren von Daten

Ein Video des Imports ist hier verfügbar.

Sie können eine Importvorschau ausführen (indem Sie das Cmdlet "Import-Policy" oder "Import-XAFarm" mit dem Preview-Parameter ausführen) und die Protokolldateien überprüfen, bevor Sie einen tatsächlichen Import ausführen.

Führen Sie die folgenden Schritte aus, um Daten mit den beim Export erstellten XML-Dateien in eine XenApp 7.6-Site zu importieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Melden Sie sich als Administrator mit Lese- und Schreibrechten und Windows-Berechtigung zum Ausführen von PowerShell-Skripts am XenApp 7.6-Controller an.
2. Wenn Sie das Paket mit dem Migrationstool (XAMigration) noch nicht in der Netzwerkfreigabe entzippt haben, führen Sie den Vorgang nun aus. Kopieren Sie die Datei ImportFMA.zip von der Netzwerkfreigabe auf den XenApp 7.6-Controller. Entzippen und extrahieren Sie ImportFMA.zip auf dem Controller in einen Ordner (z. B.: C:\XAMigration).
3. Kopieren Sie die XML-Dateien (die während des Exports erstellten Ausgabedateien) vom XenApp 6.x-Controller in den Speicherort auf dem XenApp 7.6-Controller, wo Sie die Dateien aus ImportFMA.zip extrahiert haben.
   Wenn Sie die Anwendungssymboldaten beim Ausführen des Cmdlets "Export-XAFarm" nicht in die XML-Ausgabedatei eingebettet haben, kopieren Sie den Ordner mit den Symboldaten in den gleichen Speicherort auf dem XenApp 7.6-Controller, in den Sie die XML-Ausgabedateien kopiert haben und in dem sich die extrahierten Dateien aus ImportFMA.zip befinden.
4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest.
   cd C:\XAMigration
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von Get-ExecutionPolicy.
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf "RemoteSigned" fest, damit die Skripts ausgeführt werden können. Beispiel:
   Set-ExecutionPolicy RemoteSigned
7. Importieren Sie die PowerShell-Moduldefinitionsdateien "ImportPolicy.psd1" und "ImportXAFarm.psd1":
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   **Gut zu wissen**:
   - Wenn Sie nur Richtliniendaten importieren möchten, können Sie nur die Moduldefinitionsdatei "ImportPolicy.psd1" importieren. Genauso gilt, wenn Sie nur Farmdaten importieren möchten, importieren Sie nur "ImportXAFarm.psd1".
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung .psm1.
8. Wenn Sie Richtliniendaten importieren, führen Sie das Cmdlet Import-Policy aus. Geben Sie dabei die XML-Datei mit den exportierten Richtliniendaten an.

| Parameter | Beschreibung |
|---|---|
| -XmlInputFile "<string>.xml" | Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-Policy" gesammelt wurden. Sie muss die Erweiterung .xml haben.<br><br>Standardwert: Keiner. Dieser Parameter ist erforderlich. |
| -XsdFile " <string>" | Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: PolicyData.XSD |
| -LogFile " <string>" | Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden.<br><br>Standardwert: siehe Protokollierung und Fehlerbehandlung |
| -NoLog | Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist.<br><br>Standardwert: False; Protokollausgabe wird erstellt |
| -NoClobber | Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung.<br><br>Standardwert: False; eine vorhandene Protokolldatei wird überschrieben |
| -NoDetails | Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden.<br><br>Standardwert: False; ausführliche Berichte werden an der Konsole gesendet |
| -SuppressLogo | Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Parameter | Beschreibung |
|---|---|
| | Standardwert: False; die Meldung wird auf der Konsole gedruckt |
| -Preview | Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde.<br><br>Standardwert: False; ein echter Import wird ausgeführt |

Beispiel: Mit dem folgenden Cmdlet werden Richtliniendaten aus der XML-Datei "MyPolicies.xml" importiert. Der Vorgang wird in der Datei "MyPolicies.log" protokolliert.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Wenn Sie Anwendungen importieren, führen Sie das Cmdlet Import-XAFarm aus. Geben Sie dabei eine Protokolldatei und die XML-Datei mit den exportierten Farmdaten an.

| Parameter | Beschreibung |
|---|---|
| -XmlInputFile "<string>.xml" | Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-XAFarm" gesammelt wurden. Sie muss die Erweiterung .xml haben.<br><br>Standardwert: Keiner. Dieser Parameter ist erforderlich. |
| -XsdFile "<string>" | Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: XAFarmData.XSD |
| -LogFile "<string>" | Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden.<br><br>Standardwert: siehe Protokollierung und Fehlerbehandlung |
| -NoLog | Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist.<br><br>Standardwert: False; Protokollausgabe wird erstellt |
| -NoClobber | Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung.<br><br>Standardwert: False; eine vorhandene Protokolldatei wird überschrieben |
| -NoDetails | Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden.<br><br>Standardwert: False; ausführliche Berichte werden an der Konsole gesendet |
| -SuppressLogo | Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen.<br><br>Standardwert: False; die Meldung wird auf der Konsole gedruckt |
| -Preview | Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde.<br><br>Standardwert: False; ein echter Import wird ausgeführt |
| -DeliveryGroupName "<string>" | Bereitstellungsgruppenname für alle importierten Anwendungen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Parameter | Beschreibung |
| --- | --- |
| | Standardwert: "<xenapp-farm-name> - Delivery Group" |
| -MatchFolder "<string>" | Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -NotMatchFolder "<string>" | Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) nicht übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -MatchServer "<string>" | Import von Anwendungen auf Servern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. |
| -NotMatchServer "<string>" | Import von Anwendungen auf Servern, deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -MatchWorkerGroup "<string>" | Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -NotMatchWorkerGroup "<string>" | Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -MatchAccount "<string>" | Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -NotMatchAccount "<string>" | Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.<br><br>Standardwert: Keine Übereinstimmung |
| -IncludeStreamedApps | Import von Anwendungen des Typs "StreamedToClientOrServerInstalled". (Keine anderen gestreamten Anwendungen werden importiert.)<br><br>Standard: Gestreamte Anwendungen werden nicht importiert |
| -IncludeDisabledApps | Import von Anwendungen, die als deaktiviert markiert sind.<br><br>Standard: Deaktivierte Anwendungen werden nicht importiert |

Beispiel: Das folgende Cmdlet importiert Anwendungen aus der XML-Datei "MyFarm.xml". Der Vorgang wird in der Datei "MyFarm.log" protokolliert.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"  -LogFile ".\MyFarm.Log"
```

10. Führen Sie nach dem Abschluss des Imports die nach der Migration erforderlichen Aufgaben durch.

### Aufgaben nach der Migration

Nach dem erfolgreichen Import von XenApp 6.x-Richtlinien und Farmeinstellungen in eine XenApp 7.6-Site stellen Sie mit den folgenden Richtlinien sicher, dass die Daten richtig importiert wurden.

- **Richtlinien und Richtlinieneinstellungen**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Das Importieren von Richtlinien ist im Prinzip ein Kopiervorgang mit Ausnahme von veralteten Einstellungen und Richtlinien, die nicht importiert werden. Mit der Prüfung nach der Migration werden die beiden Seiten verglichen.

1. In der Protokolldatei werden alle importierten und ignorierten Richtlinien und Einstellungen aufgeführt. Überprüfen Sie zuerst die Protokolldatei und identifizieren Sie die Einstellungen und Richtlinien, die nicht importiert wurden.
2. Vergleichen Sie die XenApp 6.x-Richtlinien mit den nach XenApp 7.6 importierten Richtlinien. Die Werte der Einstellungen sollten gleich bleiben (außer bei veralteten Richtlinieneinstellungen, siehe nächster Schritt).
   - Bei einer kleinen Anzahl von Richtlinien können Sie einen visuellen Vergleich der Richtlinien im XenApp 6.x AppCenter und in XenApp 7.6 Studio durchführen.
   - Bei einer großen Anzahl von Richtlinien ist ein visueller Vergleich u. U. nicht möglich. Verwenden Sie in solchen Fällen das Export-Cmdlet (Export-Policy), um die XenApp 7.6-Richtlinien in eine andere XML-Datei zu exportieren. Vergleichen Sie dann mit einem Textvergleichsprogramm (z. B. Windiff) die Daten der Datei mit den Daten in der XML-Datei, die zum Richtlinienexport aus XenApp 6.x verwendet wurde.
3. Der Abschnitt Nicht importierte Richtlinieneinstellungen enthält Informationen dazu, was sich beim Import geändert haben könnte. Wenn eine XenApp 6.x-Richtlinie nur veralteten Einstellungen enthält, wird die gesamte Richtlinie nicht importiert. Beispiel: Wenn eine XenApp 6.x-Richtlinie nur HMR-Testeinstellungen enthält, wird die Richtlinie vollständig ignoriert, da es keine entsprechende Einstellung in XenApp 7.6 gibt.
   Einige XenApp 6.x-Richtlinieneinstellungen werden nicht mehr unterstützt, aber vergleichbare Funktionen wurden in XenApp 7.6 implementiert. In XenApp 7.6 können Sie beispielsweise einen Neustartzeitplan für Serverbetriebssystemmaschinen konfigurieren, indem Sie eine Bereitstellungsgruppe bearbeiten. Diese Funktionalität wurde zuvor über Richtlinieneinstellungen implementiert.

4. Lesen Sie sich noch einmal durch, wie Filter in einer XenApp 7.6-Site im Gegensatz zu XenApp 6.x angewendet werden. Durch die wesentlichen Unterschiede zwischen der XenApp 6.x-Farm und der XenApp 7.6-Site kann sich die Wirkung von Filtern ändern.

- **Filter**
  Überprüfen Sie sorgfältig die Filter für die einzelnen Richtlinien. Damit sie in XenApp 7.6 weiterhin genauso funktionieren wie in XenApp 6.x, sind u. U. Änderungen erforderlich.

| Filter | Überlegungen |
|---|---|
| Zugriffssteuerung | Die Zugriffssteuerung sollte die gleichen Werte wie die ursprünglichen XenApp 6.x-Filter enthalten und ohne Änderungen funktionieren. |
| Citrix CloudBridge | Ein einfacher Boolescher Wert, der ohne Änderungen funktionieren sollte. |
| Client-IP-Adresse | Listet Client-IP-Adressbereiche auf. Jeder Bereich ist entweder zugelassen oder verweigert. Das Importskript behält die Werte bei, aber Änderungen können erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden. |
| Clientname | Ähnlich wie beim Client-IP-Adressenfilter behält das Importskript die Werte bei. Es können jedoch Änderungen erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden. |
| Organisationseinheit | Die Werte werden beibehalten, wenn die Organisationseinheiten beim Import aufgelöst werden können. Überprüfen Sie diesen Filter sorgfältig, besonders wenn die XenApp 6.x- und XenApp 7.6-Maschinen in unterschiedlichen Domänen sind. Wenn Sie die Filterwerte nicht richtig konfigurieren, wird die Richtlinie möglicherweise auf einen falschen Satz Organisationseinheiten angewendet.<br><br>Die Organisationseinheiten werden nur durch Namen dargestellt, daher ist es möglich, dass eine Organisationseinheit zu einer Organisationseinheit aufgelöst wird, die andere Mitglieder enthält als die Organisationseinheit in der XenApp 6.x-Domäne. Selbst wenn einige Werte des Organisationseinheitsfilters beibehalten werden, prüfen Sie die Werte sorgfältig. |
| Benutzer oder Gruppe | Die Werte werden beibehalten, wenn die Konten beim Import aufgelöst werden können.<br><br>Ähnlich wie Organisationseinheiten werden die Konten nur nach Namen aufgelöst. Wenn die XenApp 7.6-Site eine Domäne mit den gleichen Domänen- und Benutzernamen enthält, wobei es sich aber tatsächlich um zwei verschiedene Domänen und Benutzer handelt, entsprechen die aufgelösten Konten möglicherweise nicht den Domänenbenutzern in XenApp 6.x. Wenn Sie die Filterwerte nicht richtig überprüfen und ändern, kann es zur falschen Anwendung von Richtlinien kommen. |
| Workergruppe | Workergruppen werden in XenApp 7.6 nicht unterstützt. Verwenden Sie die Bereitstellungsgruppe, den Bereitstellungsgruppentyp und die Tagfilter, die in XenApp 7.6 unterstützt werden (nicht in XenApp 6.x).<br>• Bereitstellungsgruppe: Ermöglicht die Anwendung von Richtlinien basierend auf Bereitstellungsgruppen. Jeder Filtereintrag gibt eine Bereitstellungsgruppe an und kann zugelassen oder verweigert werden.<br>• Bereitstellungsgruppentyp: Ermöglicht die Anwendung von Richtlinien basierend auf Bereitstellungsgruppentypen. Jeder Filter |

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

| | |
|---|---|
| **Filter** | gibt einen Bereitstellungsgruppentyp an und kann zugelassen oder verweigert werden.<br>**Überlegungen**<br>• Tag: Gibt die Richtlinienanwendung basierend auf Tags an, die für VDA-Maschinen erstellt wurden. Jedes Tag kann zugelassen oder verweigert werden. |

Filter, die Domänenbenutzeränderungen umfassen, müssen besonders sorgfältig überprüft werden, wenn die XenApp 6.x-Farm in einer anderen Domäne ist als die XenApp 7.6-Site. Da das Importskript nur die Zeichenfolgen von Domänen- und Benutzernamen verwendet, um Benutzer in der neuen Domäne aufzulösen, werden einige Konten möglicherweise aufgelöst und andere nicht. Obwohl nicht sehr wahrscheinlich ist, dass verschiedene Domänen und Benutzer den gleichen Namen haben, sollten Sie unbedingt die Filter sorgfältig überprüfen, um sicherzustellen, dass sie korrekte Werte enthalten.

- **Anwendungen**
  Die Skripts zum Import von Anwendungen importieren nicht nur Anwendungen, sondern sie erstellen auch Objekte, z. B. Bereitstellungsgruppen. Wenn der Anwendungsimport mehrere Durchläufe umfasst, können sich die Originalhierarchien der Anwendungsordner erheblich ändern.
  1. Lesen Sie als Erstes die Migrationsprotokolldateien, die Informationen dazu enthalten, welche Anwendungen importiert oder ignoriert wurden und welche Cmdlets zum Erstellen der Anwendungen verwendet wurden.
  2. Für jede Anwendung gilt Folgendes:
     - Sehen Sie sich das Protokoll an und prüfen Sie, ob die grundlegenden Eigenschaften beim Importieren beibehalten wurden. Bestimmen Sie mit den Informationen unter Zuordnung von Anwendungseigenschaften, welche Eigenschaften ohne Änderungen importiert, nicht importiert oder mit den XenApp 6.x-Anwendungsdaten initialisiert wurden.
     - Überprüfen Sie die Benutzerliste. Das Importskript importiert automatisch die explizite Liste der Benutzer in die Liste "Sichtbarkeit beschränken" der Anwendung in XenApp 7.6. Stellen Sie sicher, dass die Liste unverändert ist.
  3. Anwendungsserver werden nicht importiert. Dies bedeutet, dass auf keine der importierten Anwendungen zugegriffen werden kann. Den Bereitstellungsgruppen, die diese Anwendungen enthalten, müssen Maschinenkataloge mit den Maschinen zugewiesen werden, auf denen die ausführbaren Images der veröffentlichten Anwendungen sind. Für jede Anwendung gilt Folgendes:
     - Stellen Sie sicher, dass der Name der ausführbaren Datei und das Arbeitsverzeichnis auf eine ausführbare Datei verweisen, die auf den Maschinen vorhanden ist, die der Bereitstellungsgruppe (über die Maschinenkataloge) zugewiesen sind.
     - Überprüfen Sie einen Befehlszeilenparameter (dies kann ein beliebiges Objekt sein, z. B. Dateiname, Umgebungsvariable oder der Name einer ausführbaren Datei). Stellen Sie sicher, dass der Parameter für alle Maschinen in den Maschinenkatalogen, die der Bereitstellungsgruppe zugewiesen sind, gültig ist.
- **Protokolldateien**
  Die Protokolldateien sind die wichtigsten Referenzressourcen beim Import und Export. Aus diesem Grund werden bestehende Protokolldateien standardmäßig nicht überschrieben und Standardprotokolldateien haben eindeutige Namen.

  Im Abschnitt "Protokollierung und Fehlerbehandlung" wurde bereits erwähnt, dass die Ausgabe und die Protokolldatei, die Sie erhalten, wenn Sie die verfügbaren zusätzlichen Protokollierungsfunktionen für die PowerShell-Cmdlets "Start-Transcript" und "Stop-Transcript" verwenden (sie protokollieren alles, was in die Konsole eingegeben und gedruckt wird), eine vollständige Referenz der Import- und Exportaktivitäten bieten.

  Mit den Zeitstempeln in den Protokolldateien können Sie bestimmte Probleme diagnostizieren. Wenn beispielsweise ein Export oder Import sehr lange gedauert hat, können Sie feststellen, ob eine fehlerhafte Datenbankverbindung oder das Auflösen von Benutzerkonten viel Zeit in Anspruch genommen haben.

  Aus den in den Protokolldateien aufgezeichneten Befehlen lässt sich auch ermitteln, wie manche Objekte gelesen oder erstellt werden. Beispielsweise werden zum Erstellen einer Bereitstellungsgruppe mehrere Befehle ausgeführt, und zwar nicht nur, um das Bereitstellungsgruppenobjekt selbst zu erstellen, sondern auch andere Objekte, wie die Zugriffsrichtlinienregeln, mit denen Anwendungsobjekte Bereitstellungsgruppen zugewiesen werden.

  Mit der Protokolldatei kann auch ein fehlgeschlagener Export oder Import diagnostiziert werden. Normalerweise ist in den letzten Zeilen der Protokolldatei angegeben, was den Fehler verursacht hat. Die Fehlermeldung ist ebenfalls in der Protokolldatei gespeichert. Mit der Protokolldatei und der XML-Datei zusammen können Sie bestimmen, welches Objekt an dem Fehler beteiligt war.

Nach der Überprüfung und dem Test der Migration haben Sie folgende Möglichkeiten:

1. Upgrade der XenApp 6.5-Workerserver auf aktuelle Virtual Delivery Agents (VDAs) durch Ausführen des Installers für 7.6 auf den Servern. Der Installer entfernt die XenApp 6.5-Software und installiert dann automatisch einen aktuellen VDA. Anweisungen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.
   Bei XenApp 6.0-Workerservern müssen Sie die XenApp 6.0-Software manuell vom Server deinstallieren. Danach können Sie mit dem Installer für 7.6 den aktuellen VDA installieren. Sie können mit dem Installer für 7.6 nicht automatisch die XenApp 6.0-Software entfernen.

2. Erstellen von Maschinenkatalogen (oder Bearbeiten von vorhandenen Katalogen) für die aktualisierten Worker in der neuen XenApp-Site mit Studio.
3. Hinzufügen der aktualisierten Maschinen aus dem Maschinenkatalog zu den Bereitstellungsgruppen, die die auf den VDAs für Windows-Serverbetriebssysteme installierten Anwendungen enthalten.

### Erweiterte Verwendung

Standardmäßig exportiert das Cmdlet "Export-Policy" alle Richtliniendaten in eine XML-Datei. Parallel dazu exportiert das Cmdlet "Export-XAFarm" alle Farmdaten in eine XML-Datei. Sie können mit Befehlszeilenparametern genauer steuern, was importiert und exportiert wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Teilweiser Export von Anwendungen**: Wenn Sie eine große Anzahl von Anwendungen haben und steuern möchten, wie viele in die XML-Datei exportiert werden, verwenden Sie die folgenden Parameter:
  - AppLimit: Gibt die Anzahl der zu exportierenden Anwendungen an.
  - SkipApps: Gibt die Anzahl der zu überspringenden Anwendungen an, bevor Anwendungen exportiert werden.

  Sie können beide Parameter verwenden, um große Mengen von Anwendungen in praktischen Segmenten zu exportieren. Beispiel: Wenn Sie das erste Mal "Export-XAFarm" ausführen, möchten Sie nur die ersten 200 Anwendungen exportieren und geben daher den Wert im Parameter "AppLimit" an.

  Export-XAFarm -XmlOutputFile "Apps1-200.xml"  -AppLimit "200"

  Beim nächsten Mal, wenn Sie "Export-XAFarm" ausführen, sollen die nächsten 100 Anwendungen exportiert werden. Sie verwenden den Parameter "SkipApps", um die bereits exportierten Anwendungen (die ersten 200) zu ignorieren, und exportieren mit dem Parameter "AppLimit" die nächsten 100 Anwendungen.

  Export-XAFarm -XmlOutputFile "Apps201-300.xml"  -AppLimit "100" -SkipApps "200"
- **Bestimmte Objekte nicht exportieren**: Einige Objekte brauchen nicht exportiert zu werden und können ignoriert werden. Dazu zählen besonders Objekte, die nicht importiert werden. Weitere Informationen hierzu finden Sie unter Nicht importierte Richtlinieneinstellungen und Zuordnung von Anwendungseigenschaften. Mit den folgenden Parametern können Sie den Export unnötiger Objekte verhindern:
  - IgnoreAdmins: Administratorobjekte werden nicht exportiert
  - IgnoreServers: Serverobjekte werden nicht exportiert
  - IgnoreZones: Zonenobjekte werden nicht exportiert
  - IgnoreOthers: Konfigurationsprotokollierungs-, Lastauswertungsprogramm-, Lastausgleichsrichtlinien-, Druckertreiber- und Workergruppenobjekte werden nicht exportiert
  - IgnoreApps: Anwendungen werden nicht exportiert. Hiermit können Sie andere Daten in eine XML-Ausgabedatei exportieren und dann den Export erneut ausführen, um die Anwendungen in eine andere XML-Ausgabedatei zu exportieren.

  Sie können mit diesen Parametern auch Probleme umgehen, die zum Fehlschlagen des Exports führen können. Wenn Sie beispielsweise einen fehlerhaften Server in einer Zone haben, schlägt der Export der Zone möglicherweise fehl. Wenn Sie den Parameter "IgnoreZones" verwenden, wird der Exportvorgang mit anderen Objekten fortgesetzt.

- **Bereitstellungsgruppennamen**: Wenn nicht alle Anwendungen in einer Bereitstellungsgruppe platziert werden sollen (z. B. weil verschiedene Benutzergruppen auf sie zugreifen und sie auf verschiedenen Servern veröffentlicht werden), führen Sie "Import-XAFarm" mehrmals aus und geben Sie dabei jedes Mal unterschiedliche Anwendungen und eine andere Bereitstellungsgruppe an. Sie können Anwendungen nach der Migration zwar mit PowerShell-Cmdlets von einer Bereitstellungsgruppe in eine andere verschieben, jedoch kann das Verschieben von Anwendungen durch selektives Importieren in eindeutige Bereitstellungsgruppen reduziert oder eliminiert werden.
  1. Verwenden Sie den Parameter "DeliveryGroupName" mit dem Cmdlet "Import-XAFarm". Das Skript erstellt die angegebene Bereitstellungsgruppe, wenn sie nicht vorhanden ist.
  2. Verwenden Sie die folgenden Parameter mit regulären Ausdrücken, um die Anwendungen, die in die Bereitstellungsgruppe importiert werden sollen, basierend auf Ordner, Workergruppe Benutzerkontonamen und/oder Servernamen zu filtern. Es empfiehlt sich, den regulären Ausdruck in einzelne oder doppelte Anführungszeichen zu setzen. Weitere Informationen über reguläre Ausdrücke finden Sie unter http://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.
     - MatchWorkerGroup und NotMatchWorkerGroup: Zum Beispiel bei Anwendungen, die auf Workergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen in der Workergruppe "Productivity Apps" in eine XenApp 7.6-Bereitstellungsgruppe mit demselben Namen:
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchWorkerGroup ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’
     - MatchFolder und NotMatchFolder: Zum Beispiel bei Anwendungen, die in Anwendungsordnern organisiert sind, importiert das folgende Cmdlet Anwendungen im Ordner "Productivity Apps" in eine XenApp 7.6-Bereitstellungsgruppe mit dem gleichen Namen.
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’
       Beispielsweise importiert das folgende Cmdlet Anwendungen in Ordnern, deren Name "MS Office Apps" enthält, in die Standardbereitstellungsgruppe.
       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"
     - MatchAccount und NotMatchAccount: Zum Beispiel bei Anwendungen, die für Active Directory-Benutzer oder -Benutzergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen, die für die Benutzergruppe "Finance Group" veröffentlicht wurden, in eine XenApp 7.6-Bereitstellungsgruppe mit dem Namen "Finance"
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchAccount ‘DOMAIN\\Finance Group’ –DeliveryGroupName ‘Finance’
     - MatchServer und NotMatchServer: Zum Beispiel bei Anwendungen, die auf Servern organisiert sind, importiert das folgende Cmdlet Anwendungen von Servern, deren Name nicht "Current" ist, in eine XenApp-Bereitstellungsgruppe mit dem Namen "Legacy."
       Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
- **Anpassung**: PowerShell-Programmierer können eigene Tools erstellen. Sie können z. B. das Exportskript als Bestandstool verwenden und damit die Änderungen in einer XenApp 6.x-Farm verfolgen. Sie können auch die XSD-Dateien ändern oder Ihre eigenen XSD-Dateien erstellen, um zusätzliche Daten oder Daten in unterschiedlichen Formaten in den XML-Dateien zu speichern. Sie können eine nicht standardmäßige XSD-Datei mit jedem der Import-Cmdlets angeben.

  Hinweis: Obwohl Sie Skriptdateien für bestimmte oder höhere Migrationsanforderungen ändern können, ist der Support auf unveränderte Skripts beschränkt. Der technische Support von Citrix empfiehlt, die Skripts in den Originalzustand zurückzuversetzen, um bei Bedarf erwartetes Verhalten ermitteln und Support bereitstellen zu können.

Problembehandlung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Wenn Sie PowerShell Version 2.0 verwenden und das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien oder das Citrix Common Commands Snap-In mit dem Cmdlet Add-PSSnapIn hinzugefügt haben, wird möglicherweise die folgende Fehlermeldung angezeigt, wenn Sie Cmdlets zum Exportieren oder Importieren ausführen: "Objekt verweist nicht auf eine Instanz eines Objekts". Dieser Fehler wirkt sich nicht auf die Skriptausführung aus und kann bedenkenlos ignoriert werden.
- Vermeiden Sie es, das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien in der gleichen Konsolensitzung hinzuzufügen oder zu entfernen, in der Sie die Export- und Importskriptmodule verwenden, da diese Skriptmodule das Snap-In automatisch hinzufügen. Wenn Sie das Snap-In separat hinzufügen oder entfernen, wird u. U. einer der folgenden Fehler angezeigt:
  - "Ein Laufwerk mit dem Namen 'LocalGpo' ist bereits vorhanden." Dieser Fehler tritt auf, wenn das Snap-In zweimal hinzugefügt wird. Beim Laden versucht das Snap-In, das Laufwerk "LocalGpo" bereitzustellen und meldet dann den Fehler.
  - "Es wurde kein Parameter gefunden, der dem Parameternamen 'Controller' entspricht." Dieser Fehler wird angezeigt, wenn das Snap-In nicht hinzugefügt wurde und das Skript versucht, das Laufwerk bereitzustellen. Das Skript erkennt nicht, dass das Snap-In entfernt wurde. Schließen Sie die Konsole und starten Sie eine neue Sitzung. Importieren Sie in der neuen Sitzung die Skriptmodule. Fügen Sie das Snap-In nicht separat hinzu und entfernen Sie es auch nicht separat.
- Wenn Sie beim Importieren der Module mit der rechten Maustaste auf eine PSD1-Datei klicken und dann Öffnen oder Mit PowerShell öffnen wählen, wird das Fenster der PowerShell-Konsole in schneller Abfolge geöffnet und geschlossen, bis Sie den Vorgang anhalten. Sie vermeiden diesen Fehler, indem Sie den vollständigen Namen des PowerShell-Skriptmoduls direkt im PowerShell-Konsolenfenster eingeben (z. B. Import-Module .\ExportPolicy.psd1).
- Wenn beim Ausführen eines Exports oder Imports ein Berechtigungsfehler angezeigt wird, stellen Sie sicher, dass Sie ein XenApp-Administrator mit der Berechtigung zum Lesen von Objekten (beim Export) oder zum Lesen und Erstellen von Objekten (beim Import) sind. Sie müssen auch über die erforderlichen Berechtigungen zum Ausführen von Windows-PowerShell-Skripts verfügen.
- Wenn ein Export fehlschlägt, prüfen Sie, ob die XenApp 6.x-Farm funktionsfähig ist, indem Sie die Dienstprogramme DSMAINT und DSCHECK auf dem XenApp 6.x Controller-Server ausführen.
- Wenn Sie mit den Import-Cmdlets eine Importvorschau ausführen und später bei der tatsächlichen Migration nichts importiert wird, prüfen Sie, ob Sie den Parameter "Preview" aus den Import-Cmdlets entfernt haben.

## Nicht importierte Richtlinieneinstellungen

Die folgenden Computer- und Benutzerrichtlinieneinstellungen werden nicht importiert, da sie nicht mehr unterstützt werden. Ungefilterte Richtlinien werden nie importiert. Die Features und Komponenten, die diese Einstellungen unterstützen, wurden entweder durch neue Technologien/Komponenten ersetzt oder sind aufgrund von Änderungen an Architektur oder Plattform nicht relevant.

**Nicht importierte Computerrichtlinieneinstellungen**

- Verbindungszugriffssteuerungen
- CPU-Managementserverstufe
- DNS-Adressauflösung
- Farmname
- Vollständiges Symbolcaching
- Systemüberwachung, Systemüberwachungstests
- Hostname des Lizenzservers, den Lizenzserverport
- Limit für Benutzersitzungen, Limits für Administratorsitzungen
- Lastauswertungsprogrammname
- Protokollieren von Anmeldelimitereignissen
- Maximaler Prozentsatz der Server mit Anmeldesteuerung
- Speicheroptimierung, Speicheroptimierung - Anwendungsausschlussliste, Speicheroptimierung - Intervall, Speicheroptimierung - Tag des Monats, Speicheroptimierung - Wochentag, Speicheroptimierung - Zeit
- Offlineanwendungsclient vertrauen, Ereignisprotokollierung für Offlineanwendungen, Offlineanwendungslizenzzeitraum, Offlineanwendungsbenutzer
- Eingabeaufforderung für Kennwort
- Benutzerdefinierte Neustartwarnung, Text für benutzerdefinierte Neustartwarnung, Anmeldungen vor Neustart deaktivieren (Zeit), Neustarthäufigkeit, Willkürliches Neustartintervall, Neustartbeginn, Neustartzeit, Neustartwarnungsintervall, Neustartwarnung - Startzeit, Neustartwarnung an Benutzer, Geplante Neustarts
- Spiegeln von Sitzungen *
- XML-Anfragen vertrauen (Konfiguration in StoreFront)
- Virtuelle IP - Adapteradressenfilterung, Virtuelle IP - Liste kompatibler Programme, Virtuelle IP - Erweiterte Kompatibilität, Virtuelle IP - Adapteradressenprogrammliste
- Arbeitslastname
- XenApp-Produktedition, XenApp-Produktmodell
- Port für XML-Dienst

* Ersetzt durch Windows-Remoteunterstützung

**Nicht importierte Benutzerrichtlinieneinstellungen**

- Client-COM-Ports automatisch verbinden, Client-LPT-Ports automatisch verbinden
- Client-COM-Portumleitung, Client-LPT-Portumleitung

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- Clientdruckernamen
- Limit für gleichzeitige Anmeldungen
- Eingaben in gespiegelten Verbindungen *
- Trennentimerintervall - Fortbestehen, Beendentimerintervall - Fortbestehen
- Spiegelungsversuche protokollieren *
- Benutzer bei ausstehenden Spiegelungsverbindungen benachrichtigen *
- PreLaunch-Trennentimerintervall, PreLaunch-Beendentimerintervall
- Sitzungspriorität
- Single Sign-On, Zentraler Speicher für Single Sign-On
- Benutzer, die andere Benutzer spiegeln können; Benutzer, die andere Benutzer nicht spiegeln können *

* Ersetzt durch Windows-Remoteunterstützung

### Nicht importierte Anwendungstypen

Die folgenden Anwendungstypen werden nicht importiert:
- Serverdesktops
- Inhalt
- Gestreamte Anwendungen (App-V ist die neue Methode für das Streaming von Anwendungen)

### Zuordnung von Anwendungseigenschaften

Das Importskript für Farmdaten importiert nur Anwendungen. Die folgenden Anwendungseigenschaften werden ohne Änderungen importiert.

| IMA-Eigenschaft | FMA-Eigenschaft |
|---|---|
| AddToClientDesktop | ShortcutAddedToDesktop |
| AddToClientStartMenu | ShortcutAddedToStartMenu |
| ClientFolder | ClientFolder |
| CommandLineExecutable | CommandLineExecutable |
| CpuPriorityLevel | CpuPriorityLevel |
| Beschreibung | Beschreibung |
| DisplayName | PublishedName |
| Aktiviert | Aktiviert |
| StartMenuFolder | StartMenuFolder |
| WaitOnPrinterCreation | WaitForPrinterCreation |
| WorkingDirectory | WorkingDirectory |
| FolderPath | AdminFolderName |

Hinweis: IMA und FMA haben unterschiedliche Beschränkungen bei der Länge der Ordnernamen. In IMA ist die Länge der Ordnernamen auf 256 Zeichen beschränkt, in FMA auf 64 Zeichen. Anwendungen, deren Ordnerpfad einen Ordnernamen mit mehr als 64 Zeichen enthält, werden beim Import übersprungen. Das Limit gilt nur für die Ordnernamen im Ordnerpfad. Der gesamte Ordnerpfad kann länger sein als die aufgeführten Limits. Damit Anwendungen beim Importieren nicht übersprungen werden, empfiehlt es sich, die Länge der Anwendungsordnernamen zu prüfen und bei Bedarf vor dem Export zu kürzen.
Die folgenden Anwendungseigenschaften sind standardmäßig initialisiert oder nicht initialisiert oder auf die in den XenApp 6.x-Daten bereitgestellten Werte festgelegt:

| FMA-Eigenschaft | Wert |
|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| FMA-Eigenschaft | Wert |
|---|---|
| Name | Initialisiert auf den vollständigen Pfadnamen, der die IMA-Eigenschaften "FolderPath" und "DisplayName" enthält, aber die voranstehende Zeichenfolge "Applications\" wurde gekürzt |
| ApplicationType | HostedOnDesktop |
| CommandLineArguments | Initialisiert mit den XenApp 6.x-Befehlszeilenargumenten |
| IconFromClient | Nicht initialisiert, Standardwert = false |
| IconUid | Initialisiert auf ein Symbolobjekt, das mit XenApp 6.x-Symboldaten erstellt wurde |
| SecureCmdLineArgumentsEnabled | Nicht initialisiert, Standardwert = true |
| UserFilterEnabled | Nicht initialisiert, Standardwert = false |
| UUID | Schreibgeschützt, vom Controller zugewiesen |
| Sichtbar | Nicht initialisiert, Standardwert = true |

Die folgenden Anwendungseigenschaften werden teilweise migriert:

| IMA-Eigenschaft | Anmerkungen |
|---|---|
| FileTypes | Nur in der neuen XenApp-Site existierende Dateitypen werden migriert. Dateitypen, die in der neuen Site nicht existieren, werden ignoriert. Dateitypen werden erst importiert, wenn die Dateitypen in der neuen Site aktualisiert wurden. |
| IconData | Neue Symbolobjekte werden erstellt, wenn die Symboldaten für die exportierten Anwendungen angegeben wurden. |
| Accounts | Die Benutzerkonten einer Anwendung werden zwischen der Benutzerliste für die Bereitstellungsgruppe und der Anwendung aufgeteilt. Explizite Benutzer werden zur Initialisierung der Benutzerliste für die Anwendung verwendet. Zudem wird der Benutzerliste für die Bereitstellungsgruppe das Konto "Domänenbenutzer" für die Domäne der Benutzerkonten hinzugefügt. |

Die folgenden XenApp 6.x-Eigenschaften werden nicht importiert:

| IMA-Eigenschaft | Anmerkungen |
|---|---|
| ApplicationType | Wird ignoriert. |
| HideWhenDisabled | Wird ignoriert. |
| AccessSessionConditions | Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien. |
| AccessSessionConditionsEnabled | Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien. |
| ConnectionsThroughAccessGatewayAllowed | Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien. |
| OtherConnectionsAllowed | Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien. |
| AlternateProfiles | FMA unterstützt keine gestreamten Anwendungen. |
| OfflineAccessAllowed | FMA unterstützt keine gestreamten Anwendungen. |
| ProfileLocation | FMA unterstützt keine gestreamten Anwendungen. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| IMA-Eigenschaft | Anmerkungen |
| --- | --- |
| ProfileProgramArguments | FMA unterstützt keine gestreamten Anwendungen. |
| ProfileProgramName | FMA unterstützt keine gestreamten Anwendungen. |
| RunAsLeastPrivilegedUser | FMA unterstützt keine gestreamten Anwendungen. |
| AnonymousConnectionsAllowed | FMA verwendet eine andere Technologie für die Unterstützung nicht authentifizierter (anonymer) Verbindungen. |
| ApplicationId, SequenceNumber | IMA-eigene Daten. |
| AudioType | FMA unterstützt keine erweiterten Clientverbindungsoptionen. |
| EncryptionLevel | SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert. |
| EncryptionRequired | SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert. |
| SslConnectionEnabled | FMA verwendet eine andere TLS-Implementierung. |
| ContentAddress | FMA unterstützt keinen veröffentlichten Inhalt. |
| ColorDepth | FMA unterstützt keine erweiterten Fensterformen. |
| MaximizedOnStartup | FMA unterstützt keine erweiterten Fensterformen. |
| TitleBarHidden | FMA unterstützt keine erweiterten Fensterformen. |
| WindowsType | FMA unterstützt keine erweiterten Fensterformen. |
| InstanceLimit | FMA unterstützt keine Anwendungslimits. |
| MultipleInstancesPerUserAllowed | FMA unterstützt keine Anwendungslimits. |
| LoadBalancingApplicationCheckEnabled | FMA verwendet eine andere Technologie für den Lastausgleich. |
| PreLaunch | FMA verwendet eine andere Technologie für den Sitzungsvorabstart. |
| CachingOption | FMA verwendet eine andere Technologie für den Sitzungsvorabstart. |
| ServerNames | FMA verwendet eine andere Technologie. |
| WorkerGroupNames | FMA unterstützt keine Workergruppen. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Migrieren von XenDesktop 4

Jul 08, 2016

Sie können die Daten und Einstellungen von einer XenDesktop 4-Farm in eine XenDesktop 7.x-Site mit dem Migrationstool übertragen. Dieses ist auf dem Installationsmedium im Ordner "Support > Tools > MigrationTool". Das Tool enthält Folgendes:

- Das Exporttool XdExport für den Export der XenDesktop 4-Farmdaten in eine XML-Datei (Standardname: XdSettings.xml). Das XML-Dateischema ist in der Datei XdFarm.xsd.
- Das Importtool XdImport zum Importieren der Daten unter Ausführen des PowerShell-Skripts Import-XdSettings.ps1.

Das Migrationstool kann nur verwendet werden, wenn beide Bereitstellungen dieselbe Hypervisorversion (beispielsweise XenServer 6.2) und eine Active Directory-Umgebung haben.

Sie können mit diesem Tool nicht XenApp oder XenDesktop 4 nach XenApp migrieren.

Tipp: Sie können ein Upgrade von XenDesktop 5 (oder höheren XenDesktop-Versionen) auf die aktuelle XenDesktop-Version durchführen (siehe Upgrade einer Bereitstellung).

## Einschränkungen

Nicht alle Daten und Einstellungen werden exportiert. Die folgenden Konfigurationselemente werden nicht migriert. Sie werden zwar exportiert, aber nicht importiert:

- Administratoren
- Einstellungen für delegierte Administration
- Desktopgruppenordner
- Lizenzierungskonfiguration
- Registrierungsschlüssel

Folgende Anwendungsfälle werden bei der Migration nicht direkt unterstützt:

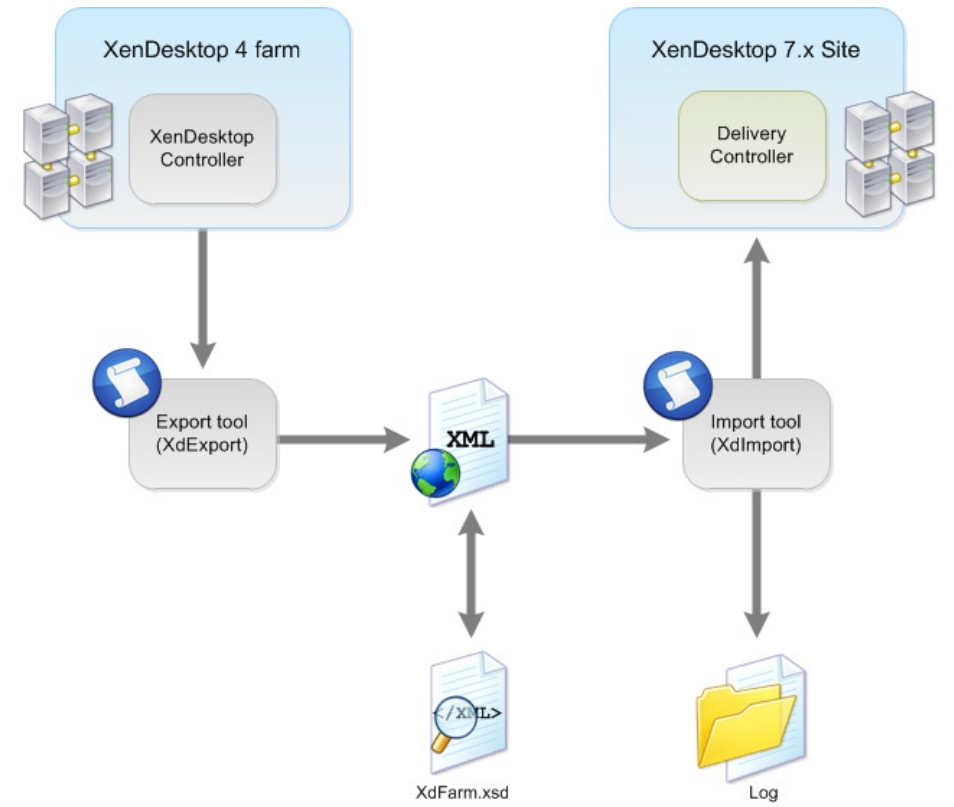
- Zusammenführen von Richtlinieneinstellungen oder Desktopgruppen- oder Hostingeinstellungen
- Zusammenführen von privaten Desktops in zufällige Bereitstellungsgruppen
- Anpassen vorhandener Komponenteneinstellungen mit Migrationstools

Weitere Informationen finden Sie unter Bei der Migration eingeschlossene und ausgeschlossene Elemente.

## Migrationsschritte

In der folgenden Abbildung wird der Migrationsvorgang zusammengefasst.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Der Migrationsprozess besteht aus folgenden Schritten:

1. Aktivieren Sie in der Studio-Konsole auf dem XenDesktop 4-Controller den Wartungsmodus für alle Maschinen, die Sie exportieren möchten.
2. Exportieren Sie Daten und Einstellungen von der XenDesktop 4-Farm mit XdExport in eine XML-Datei (siehe Exportieren aus einer XenDesktop 4-Farm).
3. Bearbeiten Sie die XML-Datei so, dass sie nur die Daten und Einstellungen enthält, die Sie in Ihre XenDesktop-Site importieren möchten (siehe Bearbeiten der XML-Datei des Migrationstools).
4. Importieren Sie die Daten und Einstellungen aus der XML-Datei mit XdImport in Ihre neue XenDesktop-Site (siehe Importieren von XenDesktop 4-Daten).
5. Wiederholen Sie die Schritte 3 und 4, um weitere Änderungen vorzunehmen. Nach dem Vornehmen von Änderungen können Sie zusätzliche Desktops in vorhandene Bereitstellungsgruppen importieren. Verwenden Sie hierzu den Mergedesktops-Parameter beim Import.
6. Führen Sie die nach der Migration erforderlichen Schritte durch (siehe Aufgaben nach der Migration).

## Vorbereitung der Migration

Führen Sie vor der Migration die folgenden Schritte durch:

- Informieren Sie sich darüber, welche Daten exportiert und importiert werden können und welche Konsequenzen dies für Ihre Bereitstellung hat. Siehe Bei der Migration eingeschlossene und ausgeschlossene Elemente.
- Citrix empfiehlt, dass Sie manuell eine Sicherungskopie der Sitedatenbank erstellen, damit Sie sie bei Problemen wiederherstellen können.
- Installieren Sie die XenDesktop 7.x-Komponenten und erstellen Sie eine Site einschließlich Datenbank.
- Für die Migration von XenDesktop 4 müssen alle VDAs auf der XenDesktop 5.x-Stufe sein, damit sie mit XenDesktop 4- und XenDesktop 7-Controllern kompatibel sind. Wenn in der Controllerinfrastruktur XenDesktop 7.x vollständig ausgeführt wird, können Windows 7-VDAs auf XenDesktop 7.x aktualisiert werden. Weitere Details finden Sie unter Migrationsbeispiele.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Exportieren aus einer XenDesktop 4-Farm

Jul 08, 2016

Das Exporttool "XdExport" extrahiert Daten aus einer einzelnen XenDesktop 4-Farm und generiert eine XML-Datei aus Darstellungen der Datenwerte.

Das Schema der XML-Datei wird in der Datei XdFarm.xsd bereitgestellt, die im Download des Importtools XdExport.zip und XdImport.zip enthalten ist.

Führen Sie XdExport auf einer Maschine aus, die in der Farm, aus der Daten exportiert werden, als XenDesktop 4-Controller fungiert. Auf dieser Maschine muss das XenDesktop 4-PowerShell SDK installiert sein. Sie müssen über die folgenden Berechtigungen für den Export der Daten verfügen:

- Die Benutzeridentität eines mindestens lesezugriffsberechtigten Citrix Administrators der Farm
- Berechtigung zum Lesen der Registrierung

Obwohl dies nicht empfohlen wird, können Sie das Tool ausführen, während der XenDesktop Controller aktiv verwendet wird (z. B. wenn Benutzer bei VDAs angemeldet sind).

Citrix empfiehlt dringend Folgendes:

- Update des XenDesktop 4-Controllers, auf dem das Tool ausgeführt wird, mit öffentlichen Hotfixes
- Keine Konfigurationsänderungen an der Site während der Export ausgeführt wird (z. B. Entfernen von Desktopgruppen)

1. Laden Sie XdExport.zip herunter und extrahieren Sie die Dateien auf den XenDesktop 4-Controller.
2. Führen Sie an einer Eingabeaufforderung XdExport.exe mit folgenden optionalen Parametern aus:

| Parameter | Beschreibung |
|---|---|
| -Verbose | Generiert Nachrichten, die detaillierte Fortschrittsinformationen liefern. |
| -FilePath <path> | Der Speicherort der XML-Datei, in die die Farmdaten exportiert werden. Standard = .\XdSettings.xml |
| -Overwrite | Überschreibt jede in -FilePath angegebene Datei. Wenn Sie diesen Parameter nicht angeben und eine Ausgabedatei bereits vorhanden ist, schlägt das Tool folgender Fehlermeldung fehl: &quot.Fehler: Datei bereits vorhanden. Geben Sie -Overwrite an, um das Überschreiben der Datei zuzulassen. " |
| -? oder -help | Zeigt eine Beschreibung der Parameter an. Beim Beenden werden keine Daten exportiert. |

3. Bei erfolgreicher Ausführung des Tools wird die Meldung Fertig angezeigt. Die Datei XdSettings.xml befindet sich an dem vom Parameter FilePath angegebenen Speicherort. Schlägt das Tool fehl, wird eine Fehlermeldung angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bearbeiten der XML-Datei des Migrationstools

Jul 08, 2016

Vor dem Importieren von Daten in eine XenDesktop 7.x-Site bearbeiten und prüfen Sie den Inhalt der vom Exporttool (XdExport) erstellten XML-Datei, besonders, wenn Sie die Migration in mehreren Phasen durchführen und beim Import einige Benutzer, Bereitstellungsgruppen und Richtlinien anderen vorgezogen haben.

Sie können den Inhalt der Datei mit einem beliebigen Texteditor anzeigen oder ändern. Sie können auch einen speziellen XML-Editor wie Microsoft XML Notepad verwenden.

Bestimmte Elemente des XML-Inhalts müssen in der XML-Datei vorhanden sein, damit sie vom Importtool (XdImport) verarbeitet wird.

Das benötigte XML-Schema ist in der Datei XdFarm.xsd definiert, die im Download des Migrationstools enthalten ist. Beim Arbeiten mit dieser Datei gilt Folgendes:

- In der Datei gibt das Attribut "minOccurs" mit einem Wert von 1 oder höher an, dass bestimmte Elemente vorhanden sein müssen, wenn das übergeordnete Element vorhanden ist.
- Wenn die an das Importtool übergebene XML-Datei ungültig ist, stoppt das Tool und eine Fehlermeldung wird angezeigt, mit deren Hilfe Sie in der XML-Datei nach dem Problem suchen können.

## Importieren einer Untergruppe von Desktops oder Bereitstellungsgruppen

Zum Importieren nur einer Untergruppe von Desktopgruppen und Desktops müssen Sie den Inhalt des Elements DesktopGroups bearbeiten. Das Element DesktopGroups kann viele DesktopGroup-Elemente enthalten und in jedem DesktopGroup-Element befindet sich ein Desktops-Element, das zahlreiche Desktop-Elemente enthalten kann.

Löschen Sie das DesktopGroups-Element nicht. Sie können aber alle DesktopGroup-Elemente löschen und es leer lassen. Ebenso muss in jedem DesktopGroup-Element das Desktops-Element vorhanden sein. Es muss aber keine Desktop-Elemente enthalten.

Löschen Sie Desktop- oder DesktopGroup-Elemente, um zu verhindern, dass bestimmte einzelne Maschinen oder ganze Bereitstellungsgruppen importiert werden. Die XML-Datei enthält beispielsweise:

… … … … … … …

Bei diesem Beispiel wird durch die Änderungen verhindert, dass die Gruppe "Group1" importiert wird. Nur Machine3 aus der Gruppe "Group2" wird importiert:

… … …

## Verwalten von Bereitstellungsgruppen mit doppelten Namen

In XenDesktop 4 können Desktopgruppen in Ordnern organisiert werden, Desktopgruppen mit dem gleichen Namen können in verschiedenen Ordnern erscheinen und der interne Name einer Desktopgruppe ist der Name, der den Benutzern angezeigt wird. In diesem Release hingegen dürfen Bereitstellungsgruppen nicht in Ordnern platziert werden und jede Bereitstellungsgruppe muss einen eindeutigen internen Namen haben, wobei der Name, der den Benutzern angezeigt wird, sich vom internen Namen unterscheiden kann. Aufgrund dieser Unterschiede müssen Sie möglicherweise Desktopgruppen umbenennen.

In Ihrer XenDesktop 4-Farm können Sie beispielsweise zwei verschiedene Desktopgruppen haben, die zwei verschiedenen Benutzern mit dem Namen "Mein Desktop" angezeigt wird. Dies kann durch Desktopgruppenordner ermöglicht werden. Wenn diese Bereitstellungsgruppen in der XenDesktop 7.x-Site getrennt bleiben sollen, müssen Sie die Namen der Desktopgruppen in der XML-Datei in eindeutige Namen ändern.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn eine Bereitstellungsgruppe in der XenDesktop 7.x-Site über denselben Namen verfügt wie die zu importierende Desktopgruppe und die Bereitstellungsgruppen in der XenDesktop 7.x-Site getrennt bleiben sollen, müssen Sie den Namen der XenDesktop 4-Desktopgruppe in der XML-Datei ändern, damit der Name in der Site eindeutig bleibt. Wenn die zu importierende Desktopgruppe tatsächlich der XenDesktop 7.x-Bereitstellungsgruppe entspricht und die Maschinen in der XML-Datei mit der vorhandenen Desktopgruppe zusammengeführt werden sollen, müssen Sie die Desktopgruppe nicht umbenennen. Geben Sie stattdessen den Parameter -MergeDesktops im Importtool an. Enthält die XML-Datei beispielsweise:

… \Sales … \Finance

Entfernen Sie die doppelten Namen wie folgt:

… \Sales … \Finance

## Verwalten von Richtlinienimports

Sie können einzelne Richtlinien aus der XML-Datei löschen und eindeutige Namen festlegen, um doppelte Richtliniennamen zu vermeiden. Das Zusammenführen von Richtlinien wird nicht unterstützt.

- Beim Import von Richtliniendaten werden entweder alle Richtlinien erfolgreich importiert oder es werden keine Richtliniendaten importiert, wenn an irgendeiner Stelle ein Fehler auftritt.
- Der Import zahlreicher Richtlinien mit umfangreichen Einstellungen kann mehrere Stunden dauern.
- Wenn Sie Richtlinien in Batches importieren, können deren ursprüngliche Prioritäten beeinträchtigt werden. Wenn Sie Richtlinien importieren, werden die relativen Prioritäten der importierten Richtlinien beibehalten. Sie erhalten jedoch eine höhere Priorität als bereits in der Site vorhandene Richtlinien. Wenn beispielsweise vier Richtlinien mit den Prioritäten 1 bis 4 in zwei Batches importiert werden sollen, sollten Sie die Richtlinien mit den Prioritäten 3 und 4 zuerst importieren, da der zweiten Gruppe automatisch eine höhere Priorität eingeräumt wird.

Zum ausschließlichen Importieren einer Untergruppe der Richtlinien in die XenDesktop 7.x-Site bearbeiten Sie den Inhalt des Policies-Elements. Das Policies-Element kann zahlreiche Policy-Elemente enthalten. Sie dürfen das Policies-Element nicht löschen. Sie können aber alle Policy-Elemente löschen und es leer lassen. Löschen Sie alle Policy-Elemente, um den Import bestimmter XenDesktop 4-Farmrichtlinien zu vermeiden. Enthält die XML-Datei beispielsweise:

… …

Wenn Sie den Import von XenDesktop 4-Richtlinien verhindern möchten, um mögliche Konflikte mit bereits in der XenDesktop 7.x-Site konfigurierten Richtlinien zu vermeiden, bearbeiten Sie die Datei, indem Sie einzelne Policy-Elemente wie folgt entfernen:

Alternativ können Sie die Datei so bearbeiten, dass die Richtlinie wie folgt mit einem anderen Namen importiert wird:

… …


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Importieren von XenDesktop 4-Daten

Jul 08, 2016

Das Importtool "XdImport" liest Einstellungen aus XenDesktop 4, die in der vom Exporttool "XdExport" erzeugten XML-Datei enthalten sind, und wendet diese Einstellungen auf eine vorhandene XenDesktop 7.x-Site an. Das Importtool verwendet das PowerShell-Skript Import-XdSettings.ps1.

Um nur eine Teilmenge der exportierten Daten anzuwenden, bearbeiten Sie die XML-Datei, bevor Sie das Importtool ausführen. Sie können beispielsweise Desktopgruppen und Richtlinien entfernen, die in der XenDesktop 7.x-Bereitstellung nicht benötigt werden. Das Importtool wird erfolgreich ausgeführt, wenn Sie ganze Elemente leer lassen. Sie können beispielsweise alle Desktopgruppen problemlos löschen. Das Tool überprüft vor dem Import der Daten immer die XML-Datei.

Führen Sie XdImport auf jeder Maschine aus, auf der alle XenDesktop 7.x-SDKs installiert sind. Sie müssen Volladministrator für XenDesktop sein, um das Tool auszuführen.

Stellen Sie vor dem Importieren sicher, dass Sie eine XenDesktop 7.x-Site einschließlich Datenbank eingerichtet haben. Citrix empfiehlt, den Import in XenDesktop 7.x durchzuführen, bevor Benutzertests oder eine allgemeine Sitekonfiguration durchgeführt werden. Führen Sie Konfigurationen nur zusammen, wenn die Site nicht verwendet wird.

1. Erstellen Sie eine XenDesktop 7.x-Site.
2. Laden Sie die Datei XdImport.zip herunter und extrahieren Sie die Dateien auf die Maschine, auf der das Tool ausgeführt werden soll.
3. Führen Sie in einer PowerShell-Sitzung Import-XdSettings.ps1 mit folgenden Parametern aus:

| Parameter | Beschreibung |
|---|---|
| -HypervisorConnectionCredentials | (erforderlich). Eine PowerShell-Hashtabelle, in der PSCredential-Instanzen Hypervisoradressen als Voraussetzung für die Erstellung von Hypervisorverbindungen<br><br>Geben Sie die Anmeldeinformationen für den Hypervisor ein, mit dem die XenDesktop 4-Farm eine Verbindung herstellt.<br><br>Für einen einzelnen Hypervisor können Sie das Argument folgendermaßen erstellen:<br><br>$credential = Get-Credential $mappings = @{"http://" =$credential} .\Import-XdSettings.ps1 -FilePath. \XdSettings.xml -HypervisorConnectionCredentials $mappi<br>Die in der Hashtabelle angegebene Adresse muss mit der Adresse in der XML-Datei genau übereinstimmen.<br><br>Beispiel: Erstellen Sie bei Verwendung eines XenServer- und eines VMware-Hypervisors folgendes Argument:<br><br>$Xencredential = Get-Credential  $VMWcredential = Get-Credential $mappings = @{"http://" = $Xencredential;"http:///SDK" = $VMWcredential} .\Import-XdSetting |
| -FilePath <path> | (Der Wert für ist erforderlich.) Der Speicherort der XML-Datei, aus der die Farmdaten importiert werden |
| -AdminAddress | Name des Controllers in der XenDesktop 7.x-Site Standard = localhost |
| -MergeDesktops | Fügt in der XML-Datei definierte Desktops Bereitstellungsgruppen in der XenDesktop 7.x-Site hinzu, deren Namen mit Gruppen in der XML-Datei übereinstimm hinzugefügt.<br><br>Wird dieser Parameter nicht angegeben, wird vorhandenen Bereitstellungsgruppen in der XenDesktop 7.x-Site kein Inhalt hinzugefügt. |
| -SkipMachinePolicy | Das Skript erstellt keine Maschinenrichtlinie mit Einstellungen auf Siteebene. Wenn Sie diesen Parameter nicht angeben und die Maschinenrichtlinie für die Site |
| -WhatIf | Führt einen Testlauf durch, um festzustellen, was an der XenDesktop 7.x-Site geändert und was ihr hinzugefügt werden würde. Wenn dieser Parameter angeg wird jedoch nicht geändert. |
| -LogFilePath <path> | Der vollständige Pfad der Protokolldatei. Das Protokoll enthält Text, der alle auf der XenDesktop 7.x-Site durchgeführten Schreibvorgänge beschreibt. Standa |
| -? oder -help | Zeigt eine Beschreibung von Parametern an. Beim Beenden werden keine Daten importiert. |

Wenn die XML-Datei Richtliniendaten enthält, werden alle Richtlinien erfolgreich importiert. Tritt jedoch an irgendeiner Stelle ein Fehler auf, werden keine Richtliniendaten importiert. Der Import zahlreicher Richtlinien mit umfangreichen Einstellungen kann mehrere Stunden dauern.

Nach Abschluss des Skripts wird die Meldung Fertig angezeigt. Nach erfolgreichem Import der Daten aus der XML-Datei können Sie weitere Import- und Exportvorgänge durchführen. Wenn Sie jedoch alle relevanten Daten importiert haben, können Sie die Aufgaben nach der Migration durchführen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Aufgaben nach der Migration

Jul 08, 2016

Nach dem erfolgreichen Importieren von Daten aus einer XenDesktop 4-Farm in eine XenDesktop 7.x-Site müssen Sie folgende Aufgaben durchführen, bevor Sie die neue Site als Produktionsumgebung nutzen können:

- Aktualisieren Sie die Virtual Delivery Agents (VDAs). Obwohl es nicht erforderlich ist, empfiehlt Citrix, dass Sie zunächst ein Upgrade der VDAs und dann erst ein Upgrade der Controller, von Studio oder von Director durchführen.
  - Windows Vista und Windows XP: Upgrade auf XenDesktop 5. 6 Feature Pack 1 Virtual Desktop Agent
  - Windows 7: Upgrade auf XenDesktop 7.x Virtual Delivery Agent.
- Erstellen Sie die Administratoren, die für die XenDesktop 7.x-Site benötigt werden.
- Citrix empfiehlt, ein Update der Benutzergeräte auf die aktuelle Version von Citrix Receiver durchzuführen, um von Hotfixes zu profitieren und Unterstützung für die aktuellen Funktionen zu erhalten.
- Ändern Sie die importierten Desktops so, dass die registrierungsbasierte Controller-Discovery verwendet wird, und verweisen Sie sie auf die XenDesktop 7.x-Controller mit einer der folgenden Methoden:
  - Entfernen Sie manuell den nicht benötigten Organisationseinheits-GUID-Eintrag aus der Registrierung und fügen Sie einen Registrierungseintrag "ListOfDDCs" hinzu.
  - Richten Sie eine Maschinenrichtlinie ein, um die Liste der Controller auf die Desktops mit der Active Directory-Richtlinie GPMC.msc zu verteilen. Sie können diese Einstellung nicht mit Studio konfigurieren.

  Registrierungsbasierte Controller-Discovery ist die Standardeinstellung für XenDesktop 7.x, Active Directory-basierte Discovery steht aber weiterhin zur Verfügung.

- Optional können Sie die folgenden Registrierungsschlüsseleinstellungen implementieren, die im Abschnitt zu den bewährten Methoden für die registrierungsbasierte Registrierung in XenDesktop unter CTX133384 beschrieben werden:
  - HeartbeatPeriodMS
  - PrepareSessionConnectionTimeoutSec
  - MaxWorkers
  - DisableActiveSessionReconnect
  - ControllersGroupGuid

  Wenn Sie dies unterlassen, werden die XenDesktop 7.x-Standardeinstellungen für diese Schlüssel verwendet.

- Deaktivieren Sie den Wartungsmodus für die importierten Maschinen, sofern diese vor dem Generieren der XML-Datei in XenDesktop 4 im Wartungsmodus waren.
- Überprüfen Sie die XenDesktop 7.x-Einstellungen, um sicherzustellen, dass sie korrekt sind, insbesondere dann, wenn Sie die XML-Datei PortICAConfig unter XenDesktop 4 geändert haben.
- Überprüfen Sie alle Migrationskomponenten, um sicherzustellen, dass die Migration erfolgreich abgeschlossen wurde.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Migrationsbeispiele

Jul 08, 2016

## Beispiel 1: Migrieren einer großen XenDesktop 4-Farm in eine XenDesktop 7-Site

In diesem Beispiel wird eine XenDesktop 4-Farm verwendet. Die XenDesktop 4-Farm hat 50 Desktopgruppen, wobei jede Gruppe durchschnittlich 100 Desktops hat. Die XenDesktop 4-Desktops werden über Provisioning Services (PVS) bereitgestellt und die Maschinen werden auf VMware ESX-Hypervisors ausgeführt. Auf allen VMs ist die XenDesktop 4-Version des VDAs installiert.

**Migrationsschritte**

1. Aktualisieren Sie alle XenDesktop 4-VDAs auf die XenDesktop 5.6 Feature Pack 1-VDA-Software. Dadurch können die VDAs sowohl beim XenDesktop 4-Controller als auch beim XenDesktop 7-Delivery Controller registriert werden.
2. Stellen Sie sicher, dass sich alle Benutzer von der XenDesktop 4-Farm abgemeldet haben.
3. Stellen Sie sicher, dass alle Maschinen in den Wartungsmodus gesetzt wurden.
4. Führen Sie das Exporttool (XdExport) auf der XenDesktop 4-Farm aus.
5. Installieren Sie XenDesktop 7-Komponenten.
   1. Erstellen Sie mit Studio eine Site im vollständigen Produktionsmodus.
   2. Ist Provisioning Services Teil der Bereitstellung, aktualisieren Sie den Provisioning Services-Server und die Provisioning Services-Agents.
   3. Aktualisieren Sie den Lizenzserver und die zugehörigen Lizenzen.
6. Entzippen Sie das Importtool (XdImport) in einem lokalen Verzeichnis auf dem XenDesktop 7-Controller.
7. Kopieren Sie die in Schritt 4 mit dem Exporttool erstellte XML-Datei (XdSettings.xml) in das lokale Verzeichnis.
8. Starten Sie in der PowerShell-Konsole des Studio-Stammknotens der XenDesktop 7-Site eine PowerShell-Sitzung.
9. Führen Sie das Importtool (XdImport) aus, sodass die Anmeldeinformationen der zugeordneten Hypervisors und der Pfad der XML-Datei übergeben werden.
10. Erstellen Sie manuell Administratoreinstellungen über den Administratorknoten in Studio neu. Informationen hierzu finden Sie unter Delegierte Administration.
11. Ändern Sie die importierten Desktops so, dass sie die registrierungsbasierte Controller-Discovery verwenden, und verweisen Sie sie auf den neuen XenDesktop 7-Controller.
12. Für VDAs unter Windows 7 empfiehlt Citrix ein Upgrade zur Verwendung von XenDesktop 7-VDAs für Windows-Desktopbetriebssysteme, damit alle neuen Features genutzt werden können.
    Nach dem Upgrade von VDAs auf XenDesktop 7 für Maschinen in einem Katalog oder einer Bereitstellungsgruppe aktualisieren Sie den Katalog und die Bereitstellungsgruppen.
13. Deaktivieren Sie den Wartungsmodus für die Bereitstellungsgruppen.
14. Konfigurieren Sie StoreFront, um die zuvor vom Webinterface bereitgestellten Desktops zur Verfügung zu stellen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

## Beispiel 2: Export einer XenDesktop 4-Farm mit teilweisem Import in eine XenDesktop 7.1-Site

In diesem Beispiel erfolgt die Migration in mehreren Schritten, wobei bei jedem Schritt ein Teil der verbleibenden Desktops migriert wird. Derzeit wird eine XenDesktop 4-Farm verwendet und eine XenDesktop 7.1-Site wurde bereits erstellt und ist im Einsatz. Die XenDesktop 4-Farm hat 50 Desktopgruppen, wobei jede Gruppe durchschnittlich 100 Desktops hat. Die XenDesktop 4-Desktops werden über Provisioning Services bereitgestellt und die Maschinen werden auf Citrix XenServer-Hypervisors ausgeführt. Auf allen VMs ist die XenDesktop 4-Version des VDAs installiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Migrationsschritte**

1. Führen Sie das Exporttool (XdExport) auf der XenDesktop 4-Farm aus.
   1. Entzippen Sie das Exporttool (XdExport) auf einem Desktop Delivery Controller in der Farm.
   2. Führen Sie das Exporttool als Citrix Administrator ohne Parameter aus.
2. Kopieren und bearbeiten Sie die resultierende XML-Datei, sodass sie nur die Gruppen und Desktops enthält, die Sie migrieren möchten.
3. Vergewissern Sie sich, dass in der XenDesktop 4-Farm sich alle Benutzer von den zu migrierenden Desktops abgemeldet haben und aktivieren Sie den Wartungsmodus für alle Desktops, die migriert werden sollen.
4. Entzippen Sie das Importtool (XdImport) in einem lokalen Verzeichnis auf dem XenDesktop 7.1-Delivery-Controller.
5. Kopieren Sie die bearbeitete XML-Datei in das lokale Verzeichnis.
6. Starten Sie in der PowerShell-Konsole des Studio-Stammknotens der XenDesktop 7.1-Site eine PowerShell-Sitzung.
7. Führen Sie das Importtool (XdImport) aus, sodass die Anmeldeinformationen der zugeordneten Hypervisors und der Pfad der XML-Datei übergeben werden.
8. Erstellen Sie manuell Administratoreinstellungen über den Administratorknoten in Studio neu. Informationen hierzu finden Sie unter "Delegierte Administration".
9. Ändern Sie die importierten Desktops so, dass sie die registrierungsbasierte Controller-Discovery verwenden, und verweisen Sie sie auf den neuen XenDesktop 7.1-Controller.
10. Aktualisieren Sie alle VDAs auf die entsprechende VDA-Software.
11. Nach dem Upgrade der gesamten VDA-Software auf XenDesktop 7 für Maschinen in einem Katalog oder einer Bereitstellungsgruppe aktualisieren Sie den Katalog und die Bereitstellungsgruppen.
12. Deaktivieren Sie den Wartungsmodus für die Bereitstellungsgruppen.
13. Konfigurieren Sie StoreFront, um die zuvor vom Webinterface bereitgestellten Desktops zur Verfügung zu stellen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bei der Migration eingeschlossene und ausgeschlossene Elemente

Jul 08, 2016

## Eingeschlossene Elemente

In der folgenden, wenn auch nicht vollständigen, Tabelle wird beschrieben, was während der Migration zu diesem Release mit den wichtigsten Daten geschieht. Sofern nicht anders angegeben, werden die jeweiligen Datentypen importiert.

| Datentyp | Hinweise |
|---|---|
| Desktopgruppen | Desktopgruppen werden in diesem Release zu Bereitstellungsgruppen. Symbole von Desktopgruppen werden nicht exportiert.<br><br>SecureIcaRequired ist auf True gesetzt, wenn DefaultEncryptionLevel in XenDesktop 4 nicht auf "Basic" festgelegt ist.<br><br>Wenn eine Desktopgruppe in der XenDesktop 4-Farm den gleichen Namen wie eine Bereitstellungsgruppe in der XenDesktop 7.x-Site hat, können Sie Desktops der XenDesktop 4-Gruppe einer Bereitstellungsgruppe mit demselben Namen in der Zielsite hinzufügen.<br><br>Geben Sie hierfür den Parameter MergeDesktops an, wenn Sie das Importtool ausführen. Die Einstellungen der XenDesktop 7.x-Bereitstellungsgruppe werden nicht mit den Einstellungen der XenDesktop 4-Gruppe überschrieben. Wenn dieser Parameter nicht angegeben wird und eine Gruppe mit demselben Namen wie eine in der XML-Datei definierte Gruppe existiert, zeigt das Tool einen Fehler an und wird angehalten, bevor Daten importiert werden. |
| Desktops | Sie können keine privaten Desktops zu zufälligen Bereitstellungsgruppen hinzufügen. Zufällige Desktops können einer statischen Bereitstellungsgruppe nicht hinzugefügt werden. |
| Maschinen | Maschinen werden in vier Maschinenkataloge importiert. Die folgenden Maschinenkataloge werden vom Importtool in der XenDesktop 7.x-Site automatisch erstellt:<br>• Importierte bestehende zufällige (für gepoolte VMs)<br>• Importierte bestehende statische (für zugewiesene VMs)<br>• Importierte physische zufällige (für gepoolte oder Blade-PC)<br>• Importierte physische statische (für private oder Blade-PC)<br><br>Alle folgenden Importe von Maschinen verwenden dieselben vier Maschinenkataloge. |
| Poolverwaltungspools | Umfasst aus mehreren Pools bestehende Pools und Einstellungen für betriebsbereite Pools, einschließlich Zeitplan.<br>• PeakBuffersizePercent ist standardmäßig auf 10 % gesetzt.<br>• OffPeakBufferSizePercent ist standardmäßig auf 10 % gesetzt.<br>• Alle nicht ausgewählten Tage in der Einstellung Business days in XenDesktop 4 werden in dieses Release als Teil des Wochenend-Energieschemas importiert.<br>• HostingXD4-Aktionszeiten werden auf die nächste volle Minute gerundet.<br>• Startzeiten werden auf die nächste volle Stunde gerundet.<br>• Endzeiten werden auf die nächste volle Stunde gerundet. |
| Farmeinstellungen | Die folgenden Farmeinstellungen werden als Maschinenrichtlinie importiert:<br>• IcaKeepAlive<br>• AutoClientReconnect |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Datentyp | Hinweise |
|---|---|
| | • SessionReliability<br>Die Einstellung zum Aktivieren von Flash Player wird nicht importiert. |
| Richtlinien | Bestimmte Richtliniendaten werden importiert. Filter, Einstellungen und Drucker werden als Benutzerrichtlinien importiert. Weitere Informationen zum Export und Import von Benutzerrichtlinien finden Sie in der anderen Tabelle in diesem Dokument.<br>• Neue Regeln für Zugriffsrichtlinien werden basierend auf XenDesktop 4-Gruppeneinstellungen erstellt.<br>• Beim Import von Richtlinien wird deren relative Prioritätsreihenfolge beibehalten. Sie werden jedoch immer mit einer höheren Priorität als alle auf der XenDesktop 7.x-Site vorhandenen Richtlinien hinzugefügt.<br>• Das Zusammenführen von Richtlinien wird nicht unterstützt.<br><br>Es gibt keine Möglichkeit, Richtlinien in Active Directory zu importieren. Sie werden immer in der Site gespeichert. |
| Benutzerzuweisungen | |
| Hypervisoreinstellungen | Dieser Parameter ist für das XdImport-Tool erforderlich.<br><br>Hypervisoradressen werden exportiert, nicht aber die Anmeldeinformationen, die für den Zugriff auf diese Hypervisors erforderlich sind. Zum Erstellen von Hypervisorverbindungen in der XenDesktop 7.x-Site müssen Sie die Adressen aus der XML-Datei extrahieren und eine PowerShell-Hashtabelle anlegen, in der die Adressen den entsprechenden Anmeldeinformationen zugeordnet sind. Geben Sie dann diese Tabelle im Parameter HypervisorConnectionCredentials des Importtools an. Weitere Informationen finden Sie unter Importieren von XenDesktop 4-Daten.<br><br>Das Zusammenführen oder Aktualisieren von Hypervisoreinstellungen für vorhandene Desktopgruppen und Hypervisorverbindungen wird nicht unterstützt. |
| Administratoren | (Wird nicht importiert.) Es werden keine Administratordaten importiert, einschließlich Daten über delegierte Administratoren. Sie müssen neue Administratoren für die XenDesktop 7.x-Site erstellen. |
| Lizenzierungskonfiguration | (Wird nicht importiert.) Enthält Informationen wie Lizenzservername und Edition. Lizenzdateien werden nicht exportiert. |
| Desktopgruppenordner | (Wird nicht importiert.) Dieses Release unterstützt keine Desktopgruppenordner. Bei doppelten Desktopgruppennamen (weil unterschiedliche Ordner in der XenDesktop 4-Farm Gruppen mit identischen Namen enthielten) wird das Importtool angehalten, wenn Sie die Namen in der XML-Datei nicht bearbeiten. |
| Registrierungsschlüssel | (Wird nicht importiert.) Weitere Informationen zur Implementierung von Registrierungsschlüsseln finden Sie unter Aufgaben nach der Migration. |

### Benutzerrichtliniendaten

In der folgenden Tabelle wird beschrieben, wie Benutzerrichtliniendaten exportiert und importiert werden.

| Kategorie und Einstellung in XenDesktop 4 | XML-Datei | Kategorie und Einstellung in XenDesktop 7.x |
|---|---|---|
| Bandbreite\Visuelle Effekte\Sitzungslimits<br><br>OEM-Virtuelle Kanäle | ClientOEMVCBandwidth | Nicht importiert |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Kategorie und Einstellung in XenDesktop 4 | XML-Datei | Kategorie und Einstellung in XenDesktop 7.x |
|---|---|---|
| Kategorie und Einstellung in XenDesktop 4<br><br>OEM-Virtuelle Kanäle deaktivieren | DisableOEMVirtualChannels | |
| Benutzerarbeitsbereich\Zeitzone<br><br>Lokale Zeit des Clients nicht verwenden | DoNotUseClientLocalTime | Nicht importiert |
| Sicherheit\Verschlüsselung<br><br>SecureICA-Verschlüsselung | ClientSecurityRequirement | Nicht importiert |
| Bandbreite\SpeedScreen<br><br>Beschleunigung der Bildanzeige durch verlustreiche Komprimierung | LossyCompression settings | ICA\Visuelle Anzeige\Festbilder<br><br>Grad der verlustreichen Komprimierung<br><br>Schwellenwert für verlustreiche Komprimierung<br><br>Heavyweight-Komprimierung<br><br>ICA\Visuelle Anzeige\Bewegtbilder<br><br>Grad der progressiven Komprimierung<br><br>Schwellenwert für progressive Komprimierung |
| Bandbreite\Visuelle Effekte<br><br>Desktophintergrund deaktivieren | TurnOffWallpaper | ICA\Desktopbenutzeroberfläche<br><br>Desktophintergrund |
| Bandbreite\Visuelle Effekte<br><br>Menüanimation | TurnOffMenuWindowAnimation | ICA\Desktopbenutzeroberfläche<br><br>Menüanimation |
| Bandbreite\Visuelle Effekte<br><br>Fensterinhalt beim Verschieben nicht anzeigen | DoNotShowWindowContentsWhileDragging | ICA\Desktopbenutzeroberfläche<br><br>Fensterinhalt beim Verschieben anzeigen |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br><br>Audio | ClientAudioBandwidth__AllowedBandWidth | ICA\Bandbreite<br><br>Bandbreitenlimit für die Audioumleitung |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br><br>Zwischenablage | ClientClipboardBandwidth__AllowedBandWidth | ICA\Bandbreite<br><br>Bandbreitenlimit für Zwischenablagenumleitung |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Kategorie und Einstellung in XenDesktop 4 | XML-Datei | Kategorie und Einstellung in XenDesktop 7.x |
|---|---|---|
| Bandbreite\Visuelle Effekte\Sitzungslimits<br>COM-Ports | ClientComBandwidth__AllowedBandWidth | ICA\Bandbreite<br>Bandbreitenlimit für COM-Portumleitung<br>In XenDesktop 7.0 bis 7.8 nicht importiert |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br>Laufwerke | ClientDriveBandwidth__AllowedBandWidth | ICA\Bandbreite<br>Bandbreitenlimit für Dateiumleitung |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br>LPT-Ports | ClientLptBandwidth__AllowedBandWidth | ICA\Bandbreite<br>Bandbreitenlimit für LPT-Portumleitung<br>In XenDesktop 7.0 bis 7.8 nicht importiert |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br>Sitzung insgesamt | OverallBandwidth__AllowedBandWidth | ICA\Bandbreite<br>Bandbreitenlimit für Sitzung insgesamt |
| Bandbreite\Visuelle Effekte\Sitzungslimits<br>Drucker | LimitPrinterBandWidth__AllowedBandWidth | ICA\Bandbreite<br>Bandbreitenlimit für Druckerumleitung |
| Clientgeräte\Ressourcen\Audio<br>Mikrofone | ClientAudioMicrophone__TurnOn | ICA\Audio<br>Clientmikrofonumleitung |
| Clientgeräte\Ressourcen\Audio<br>Tonqualität | ClientAudioQuality__Quality | ICA\Audio<br>Audioqualität |
| Clientgeräte\Ressourcen\Audio<br>Lautsprecher deaktivieren | DisableClientAudioMapping | ICA\Audio<br>Clientaudioumleitung |
| Clientgeräte\Ressourcen\Laufwerke<br>Verbindung (Connection) | ConnectClientDriveAtLogon__TurnOn | ICA\Dateiumleitung<br>Laufwerke automatisch verbinden |
| Clientgeräte\Ressourcen\Laufwerke<br>Diskettenlaufwerke deaktivieren | DisableClientDriveMapping__DisableFloppyDrive | ICA\Dateiumleitung<br>Clientdiskettenlaufwerke |
| Clientgeräte\Ressourcen\Laufwerke | DisableClientDriveMapping__DisableHardDrive | ICA\Dateiumleitung |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Festplatten deaktivieren<br>**Kategorie und Einstellung in XenDesktop 4** | **XML-Datei** | Lokale Clientfestplattenlaufwerke<br>**Kategorie und Einstellung in XenDesktop 7.x** |
|---|---|---|
| Clientgeräte\Ressourcen\Laufwerke<br>CD-ROM-Laufwerke deaktivieren | DisableClientDriveMapping__DisableCdrom | ICA\Dateiumleitung<br>Optische Clientlaufwerke |
| Clientgeräte\Ressourcen\Laufwerke<br>Remotelaufwerke deaktivieren | DisableClientDriveMapping__DisableRemote | ICA\Dateiumleitung<br>Clientnetzlaufwerke |
| Clientgeräte\Ressourcen\Laufwerke<br>USB-Laufwerke deaktivieren | DisableClientDriveMapping__DisableUSB | ICA\Dateiumleitung<br>Clientwechsellaufwerke |
| Clientgeräte\Ressourcen\Laufwerke\Optimierung<br>Asynchrones Schreiben | CDMAsyncWrites | ICA\Dateiumleitung<br>Asynchrones Schreiben verwenden |
| Clientgeräte\Ressourcen\Sonstiges<br>Zwischenablagezuordnung deaktivieren | DisableClientClipboardMapping | ICA<br>Clientzwischenablagenumleitung |
| Clientgeräte\Ressourcen\Ports<br>COM-Ports deaktivieren | DisableClientCOMPortMapping | ICA\Dateiumleitung<br>Client-COM-Portumleitung<br>In XenDesktop 7.0 bis 7.8 nicht importiert |
| Clientgeräte\Ressourcen\Ports<br>LPT-Ports deaktivieren | DisableClientLPTPortMapping | ICA\Dateiumleitung<br>Client-LPT-Portumleitung<br>In XenDesktop 7.0 bis 7.8 nicht importiert |
| Clientgeräte\Ressourcen\USB<br>USB | RemoteUSBDevices__DisableRemoteUSBDevices | ICA\USB-Geräte<br>Client-USB-Geräteumleitung |
| Drucken\Clientdrucker<br>Automatische Erstellung | ConnectClientPrinterAtLogon__Flag | ICA\Drucken\Clientdrucker<br>Clientdrucker automatisch erstellen |
| Drucken\Clientdrucker<br>Legacy-Clientdrucker | LegacyClientPrinters__TurnOn | ICA\Drucken\Clientdrucker<br>Clientdruckernamen |
| Drucken\Clientdrucker | ModifiedPrinterProperties__WriteMethod | ICA\Drucken\Clientdrucker |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Kategorie und Einstellung in XenDesktop 4 | XML-Datei | Kategorie und Einstellung in XenDesktop 7.x |
|---|---|---|
| Speicherung von Druckereigenschaften | | Speicherung von Druckereigenschaften |
| Drucken\Clientdrucker<br><br>Weiterleiten von Druckaufträgen | ClientPrintingForNetworkPrinter__TurnOn | ICA\Drucken\Clientdrucker<br><br>Direkte Verbindungen zu Druckservern |
| Drucken\Clientdrucker<br><br>Clientdruckerzuordnung deaktivieren | DisableClientPrinterMapping | ICA\Drucken<br><br>Clientdruckerumleitung |
| Drucken\Treiber<br><br>Native Druckertreiber automatisch installieren | PrintDriverAutoInstall__TurnOn | ICA\Drucken\Treiber<br><br>Automatische Installation von mitgelieferten Druckertreibern |
| Drucken\Treiber<br><br>Universeller Treiber | ClientPrintDriverToUse | ICA\Drucken\Treiber<br><br>Verwendung universeller Druckertreiber |
| Drucken\Sitzungsdrucker<br><br>Sitzungsdrucker | NetworkPrinters | ICA\Drucken<br><br>Sitzungsdrucker |
| Drucken\Sitzungsdrucker<br><br>Standarddrucker des Clients wählen | DefaultToMainClientPrinter__NetworkDefault<br><br>DefaultToMainClientPrinter__TurnOn | ICA\Drucken<br><br>Standarddrucker |

### Ausgeschlossene Elemente

Nicht alle XenDesktop 4-Komponenten werden in diesem Release unterstützt. Die folgenden Elemente werden nicht migriert:

- **Virtual Delivery Agent**: Bevor Sie mit einem XenDesktop 7.x-Delivery Controller virtuelle Desktops von XenDesktop 4 verwalten können, müssen Sie ein Upgrade der VDAs auf mindestens XenDesktop 5.x durchführen.
- **Controller**: Sie müssen neue Controller-Server bereitstellen. Sie können einen XenDesktop 4-Controller nicht auf eine XenDesktop 7.x-Site aktualisieren. XenDesktop 7.x-Sites können keiner XenDesktop 4-Farm und XenDesktop 4-Controller können keiner XenDesktop 7.x-Site beitreten. Darüber hinaus gelten für jede Version andere Serveranforderungen. XenDesktop 4 erfordert Windows Server 2003 und XenDesktop 7.x neuere Windows Server-Versionen.
- **Webinterface**: Citrix empfiehlt die Verwendung von StoreFront mit XenDesktop 7.x Informationen zu Installation und Einrichtung finden Sie in der StoreFront-Dokumentation. Wenn das XenDesktop-Installationsprogramm das Webinterface erkennt, wird StoreFront zwar installiert, das Webinterface jedoch nicht entfernt.
- **Konfiguration der Organisationseinheiten in Active Directory**: Die Freigabe einer Organisationseinheit zwischen zwei Farmen oder zwei Sites oder einer Farm und einer Site wird nicht unterstützt. Wenn Sie die neue Site mit der Active Directory-basierten Controller-Discovery statt der standardmäßigen registrierungsbasierten Controller-Discovery konfigurieren, müssen Sie eine neue Organisationseinheit hierfür erstellen.
- **XML-Datei PortICAConfig**: Wenn Sie die Standardeinstellungen für diese Datei geändert haben, müssen Sie diese Einstellungen für die neue Site unter Umständen über Gruppenrichtlinienobjekte konfigurieren.
- **Über XenDesktop 4 Service Pack 1 bereitgestellte Einstellungen für die Konfigurationsprotokollierung**:
- **Daten von Provisioning Services**:
- **Anwendungen**:
- **Liste der Controller**:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **NetScaler Gateway**:
- **Drosselungseinstellungen für das Ereignisprotokoll**:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sicherheit

Jul 08, 2016

XenApp und XenDesktop bieten eine auf Sicherheit ausgelegte Lösung, mit der Sie Ihre Umgebung Ihren Sicherheitsanforderungen anpassen können.

Bei mobilen Mitarbeitern steht die IT-Abteilung dem Sicherheitsrisiko durch verlorene oder gestohlene Daten gegenüber. Durch Hosten von Anwendungen und Desktops trennen XenApp und XenDesktop sicher vertrauliche Daten und geistiges Eigentum von Endpunktgeräten, da alle Daten in einem Datencenter gespeichert werden. Wenn Richtlinien für das Zulassen von Datenübertragungen aktiviert sind, werden alle Daten verschlüsselt.

Die XenDesktop- und XenApp-Datencenter vereinfachen auch die Reaktion auf Vorfälle mit einem zentralisierten Überwachungs- und Verwaltungsdienst. Mit Director überwachen und analysieren IT-Mitarbeiter Daten, auf die im Netzwerk zugegriffen wird, und mit Studio kann die IT-Abteilung im Datencenter Patches anwenden und Systemanfälligkeiten verhindern statt Probleme lokal auf jedem Endbenutzergerät zu beheben.

XenApp und XenDesktop vereinfachen auch Audits und die Einhaltung der Richtlinientreue, da Untersuchende mit einer zentralisierten Überwachungsliste ermitteln können, wer auf welche Anwendungen und Daten zugegriffen hat. Director sammelt durch Zugriff auf die Konfigurationsprotokollierung und die OData-API Verlaufsdaten über Updates des Systems und der Benutzerdatennutzung.

Mit der delegierten Administration richten Sie Administratorrollen ein, um den Zugriff auf XenDesktop und XenApp auf granulärer Ebene zu steuern. Dies ermöglicht Flexibilität in Ihrer Organisation, um bestimmten Administratoren vollständigen Zugriff auf Aufgaben, Vorgänge und Geltungsbereiche zugeben, während der Zugriff anderer Administratoren beschränkt ist.

Mit XenApp und XenDesktop wenden Administratoren Richtlinien auf verschiedenen Netzwerkebenen an, von der lokalen Ebene bis zur Organisationseinheitsebene, und steuern damit Benutzer granulär. Diese Steuerung der Richtlinien legt fest, ob ein Benutzer, ein Gerät oder eine Gruppe von Benutzern und Geräten eine Verbindung herstellen, Kopieren bzw. Einfügen oder lokale Laufwerke zuordnen können. Dies verringert Sicherheitsbedenken bei Zeitpersonal von Drittanbietern. Administratoren können auch Desktop Lock verwenden, sodass Benutzer nur den virtuellen Desktop verwenden können und der Zugriff auf das lokale Betriebssystem des Endbenutzergeräts verhindert wird.

Administratoren können die Sicherheit in XenApp oder XenDesktop erhöhen und die Site so konfigurieren, dass sie das TLS-Sicherheitsprotokoll (Transport Layer Security) des Controllers oder zwischen Endbenutzern und VDAs verwendet. Das Protokoll kann auch für eine Site aktiviert werden, um die Serverauthentifizierung, die Verschlüsselung des Datenstroms und die Prüfung der Nachrichtenintegrität für eine TCP/IP-Verbindungen bereitzustellen.

XenApp und XenDesktop unterstützen auch die mehrstufige Authentifizierung für Windows oder eine bestimmte Anwendung. Mit der mehrstufigen Authentifizierung können auch alle Ressourcen, die von XenApp und XenDesktop bereitgestellt werden, verwaltet werden. Diese Methoden sind u. a.:

- Tokens
- Smartcards
- RADIUS
- Kerberos
- Biometrie


© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenDesktop kann mit vielen Sicherheitslösungen von Drittanbietern integriert werden, von der Identitätsverwaltung bis zu Antivirensoftware. Eine Liste der unterstützten Produkte finden Sie unter http://www.citrix.com/ready.

Bestimmte Releases von XenApp und XenDesktop sind für Common Criteria zertifiziert. Eine Liste dieser Standards finden Sie unter http://www.commoncriteriaportal.org/cc/.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sicherheit – Überlegungen und bewährte Methoden

Aug 17, 2016

In diesem Dokument wird Folgendes beschrieben:

- Allgemeine bewährte Methoden zur Gewährleistung der Sicherheit beim Verwenden dieses Releases sowie sicherheitsrelevante Unterschiede zwischen diesem Release und einer konventionellen Computerumgebung
- Verwalten von Benutzerkonten
- Verwalten von Benutzerprivilegien
- Verwalten von Anmelderechten
- Konfigurieren von Benutzerrechten
- Konfigurieren von Diensteinstellungen
- Bereitstellungsszenarios und ihre Auswirkungen auf die Sicherheit
- Sicherheitsüberlegungen für Remote-PC-Zugriff

Möglicherweise muss Ihre Organisation bestimmte Sicherheitsstandards einhalten, um den gesetzlichen Anforderungen zu genügen. In diesem Dokument wird dieses Thema nicht behandelt, da sich Sicherheitsstandards mit der Zeit ändern. Aktuelle Informationen über Sicherheitsstandards und Citrix Produkte finden Sie unter http://www.citrix.com/security/.

# Bewährte Methoden zur Gewährleistung der Sicherheit

Halten Sie stets alle Computer in der Umgebung mit Sicherheitspatches auf dem neuesten Stand. Ein Vorteil besteht darin, dass Thin Clients als Terminals verwendet werden können. Das erleichtert diese Aufgabe.

Schützen Sie alle Maschinen in der Umgebung mit Antivirensoftware.

Erwägen Sie plattformspezifische Antischadsoftware, wie z. B. das Microsoft Enhanced Mitigation Experience Toolkit (EMET) für Windows-Maschinen. Manche Organisationen empfehlen, die neueste von Microsoft unterstützte Version von EMET in ihren regulierten Umgebungen zu verwenden. Beachten Sie, dass gemäß Microsoft EMET mit mancher Software nicht kompatibel ist. Es muss also gründlich mit Ihren Anwendungen getestet werden, bevor es in einer Produktionsumgebung bereitgestellt wird. XenApp und XenDesktop wurden mit EMET 5.5 in der Standardkonfiguration getestet. Derzeit wird EMET nicht für die Verwendung auf einer Maschine empfohlen, auf der ein Virtual Delivery Agent (VDA) installiert ist.

Schützen Sie alle Maschinen in der Umgebung mit Umkreisfirewalls, u. a. bei Bedarf auch an Grenzen von Enklaven.

Wenn Sie eine konventionelle Umgebung zu diesem Release migrieren, müssen Sie ggf. eine vorhandene Umkreisfirewall neu positionieren oder neue Umkreisfirewalls hinzufügen. Beispiel: Zwischen einem konventionellen Client und einem Datenbankserver im Datenzentrum befindet sich eine Umkreisfirewall. Bei diesem Release muss diese Umkreisfirewall so platziert werden, dass sich der virtuelle Desktop und das Benutzergerät auf der einen Seite befinden und die Datenbankserver und Controller im Datencenter auf der anderen Seite. Es empfiehlt sich daher, im Datencenter einen Netzbereich für die von XenDesktop verwendeten Datenbankserver und Controller zu erstellen. Außerdem sollten Sie die Installation eines Schutzmechanismus zwischen dem Benutzergerät und dem virtuellen Desktop in Betracht ziehen.

Alle Maschinen in der Umgebung müssen durch eine persönliche Firewall geschützt werden. Wenn Sie Kernkomponenten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

und VDAs installieren, können Sie die erforderlichen Ports für Komponenten und Features so einrichten, dass sie automatisch geöffnet werden, sobald der Windows-Firewalldienst erkannt wird (auch wenn die Firewall nicht aktiviert ist). Sie können die Firewallports auch manuell konfigurieren. Wenn Sie eine andere Firewall verwenden, muss diese manuell konfiguriert werden.

**Hinweis:** Da die TCP-Ports 1494 und 2598 für ICA und CGP verwendet werden, sind sie normalerweise an der Firewall geöffnet, damit Benutzer außerhalb des Rechenzentrums auf sie zugreifen können. Citrix empfiehlt, dass diese Ports nicht für etwas Anderes verwendet werden, damit administrative Benutzeroberflächen nicht versehentlich gefährdet werden. Die Ports 1494 und 2598 sind bei der Internet Assigned Numbers Authority (http://www.iana.org/) offiziell registriert.

Die gesamte Netzwerkkommunikation sollte Ihren Sicherheitsrichtlinien gemäß angemessen gesichert und verschlüsselt werden. Sie können die gesamte Kommunikation zwischen Microsoft Windows-Computern mit IPSec sichern. Weitere Informationen hierzu finden Sie in der Dokumentation zum Betriebssystem. Die Kommunikation zwischen Benutzergeräten und Desktops ist außerdem mit Citrix SecureICA gesichert, das in der Standardeinstellung 128-Bit-Verschlüsselung verwendet. Sie können beim Erstellen oder Aktualisieren einer Bereitstellungsgruppe SecureICA konfigurieren.

Übernehmen Sie die für Windows empfohlenen bewährten Methoden bei der Benutzerkontenverwaltung. Erstellen Sie kein Konto auf einer Vorlage oder einem Image, bevor dieses durch Maschinenerstellungsdienste (MCS) oder Provisioning Services dupliziert wurde. Planen Sie keine Aufgaben mit gespeicherten privilegierten Domänenkonten. Erstellen manuell Sie keine freigegebenen Active Directory-Computerkonten. Durch diese Vorgehensweise wird verhindert, dass ein lokales permanentes Kontokennwort für einen Angriff unter Anmeldung bei mit MCS bzw. PVS freigegebenen Images Anderer verwendet wird.

# Verwalten von Benutzerkonten

Wenn Sie bei der Installation eines Virtual Delivery Agents (VDA) die Option zum Installieren von App-V-Veröffentlichungskomponenten wählen oder diese Komponenten später installieren, wird dem VDA das lokale Administratorkonto CtxAppVCOMAdmin hinzugefügt. Wenn Sie die App-V-Veröffentlichung verwenden, ändern Sie dieses Konto nicht. Wenn Sie die App-V-Veröffentlichung nicht benötigen, aktivieren Sie das Feature bei der Installation nicht. Wenn Sie sich nach der Installation der App-V-Veröffentlichung gegen eine Verwendung des Features entscheiden, können Sie das Konto deaktivieren oder löschen.

# Verwalten von Benutzerprivilegien

Geben Sie Benutzern nur die Rechte, die sie benötigen. Microsoft Windows-Privilegien können weiterhin in der üblichen Weise auf Desktops angewendet werden: Konfigurieren Sie Privilegien mit "Zuweisung von Benutzerrechten" und Gruppenmitgliedschaften mit einer Gruppenrichtlinie. Der Vorteil dieses Release besteht darin, dass einem Benutzer Administratorrechte für einen Desktop eingeräumt werden können, ohne ihm auch die physische Kontrolle über den Computer, auf dem der Desktop gespeichert ist, zu gewähren.

Beachten Sie beim Planen von Desktopprivilegien Folgendes:

- Standardmäßig wird nicht berechtigten Benutzern beim Herstellen einer Verbindung mit einem Desktop die Zeitzone des Systems, auf dem der Desktop ausgeführt wird, statt der Zeitzone ihres eigenen Benutzergerätes angezeigt. Weitere Informationen dazu, wie Sie Benutzern erlauben, ihre Ortszeit beim Verwenden von Desktops anzuzeigen, finden Sie im Artikel "Verwalten von Bereitstellungsgruppen".

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- Ein Benutzer mit Administratorrechten auf einem Desktop hat Vollzugriff auf diesen Desktop. Wenn ein Desktop ein gepoolter Desktop und kein dedizierter Desktop ist, muss dem Benutzer von allen anderen Benutzern dieses Desktops, einschließlich zukünftiger Benutzer, vertraut werden. Alle Benutzer des Desktops müssen sich des potenziellen permanenten Risikos für ihre Datensicherheit bewusst sein, die diese Situation mit sich bringt. Diese Überlegung trifft nicht auf dedizierte Desktops zu, die nur einen einzelnen Benutzer haben. Dieser Benutzer sollte kein Administrator auf einem anderen Desktop sein.
- Ein Benutzer mit Administratorrechten auf einem Desktop kann auf diesem Desktop generell Software installieren, einschließlich potenziell schädlicher Software. Zudem kann der Benutzer u. U. den Datenverkehr in allen mit dem Desktop verbundenen Netzwerken überwachen und steuern.

# Verwalten von Anmelderechten

Geben Sie Benutzern die erforderlichen Anmelderechte. Wie Microsoft Windows-Privilegien werden Anmelderechte weiterhin in der üblichen Weise auf Desktops angewendet: Konfigurieren Sie Anmelderechte mit "Zuweisung von Benutzerrechten" und Gruppenmitgliedschaften mit einer Gruppenrichtlinie.

Es gibt folgende Windows-Anmelderechte: Lokal anmelden, Anmelden über Remotedesktopdienste, Übers Netzwerk anmelden, Anmelden als Stapelverarbeitungsauftrag und Anmelden als Dienst.

Laut Microsoft wird der Gruppe Remotedesktopbenutzer standardmäßig das Anmelderecht "Anmelden über Remotedesktopdienste" gewährt (außer für Domänencontroller).

Die Sicherheitsrichtlinie Ihres Unternehmens legt möglicherweise explizit fest, dass diese Gruppe aus dem Anmelderecht entfernt werden sollte. Erwägen Sie folgenden Ansatz:

- Der Virtual Delivery Agent (VDA) für Serverbetriebssysteme verwendet Microsoft-Remotedesktopdienste. Sie können die Gruppe der Remotedesktopbenutzer als eine eingeschränkte Gruppe konfigurieren und die Gruppenmitgliedschaft durch Active Directory-Gruppenrichtlinien steuern. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Für andere XenApp- und XenDesktop-Komponenten, einschließlich dem VDA für Desktopbetriebssysteme, ist die Gruppe der Remotedesktopbenutzer nicht erforderlich. Für diese Komponenten benötigt die Gruppe der Remotedesktopbenutzer das Recht "Anmelden über Remotedesktopdienste" also nicht und Sie können es entfernen. Beachten Sie außerdem Folgendes:
  - Wenn Sie diese Computer mit Remotedesktopdienste verwalten, stellen Sie sicher, dass alle Administratoren Mitglieder der Administratorgruppe sind.
  - Wenn Sie diese Computer nicht mit Remotedesktopdienste verwalten, könnten Sie Remotedesktopdienste auf diesen Computern deaktivieren.

Es ist zwar möglich, dem Anmelderecht "Anmelden über Remotedesktopdienste verweigern" Benutzer und Gruppen hinzuzufügen, jedoch wird von der Verwendung von verweigernden Rechten allgemein abgeraten. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

# Konfigurieren von Benutzerrechten

Bei der Installation des Delivery Controllers werden die folgenden Windows-Dienste erstellt:

- Citrix AD-Identitätsdienst (NT SERVICE\CitrixADIdentityService): Verwaltet Microsoft Active Directory-Computerkonten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

für VMs.

- Citrix Analytics (NT SERVICE\CitrixAnalytics): Sammelt Sitekonfigurations- und Nutzungsinformationen zur Verwendung von Citrix, wenn das Sammeln vom Siteadministrator genehmigt wurde. Diese Informationen werden dann an Citrix gesendet, damit das Produkt verbessert werden kann.
- Citrix App-Bibliothek (NT SERVICE\CitrixAppLibrary): Unterstützt die Verwaltung und das Provisioning von AppDisks, AppDNA-Integration und die Verwaltung von App-V.
- Citrix Brokerdienst (NT SERVICE\CitrixBrokerService): Wählt die virtuellen Desktops oder Anwendungen aus, die den Benutzern zur Verfügung stehen.
- Citrix Konfigurationsprotokollierungsdienst (NT SERVICE\CitrixConfigurationLogging): Erfasst alle Konfigurationsänderungen und andere Zustandsänderungen, die von den Administratoren an der Site vorgenommen werden.
- Citrix Konfigurationsdienst (NT SERVICE\CitrixConfigurationService): Repository der Site für freigegebene Konfigurationen.
- Citrix Dienst für die delegierte Administration (NT SERVICE\CitrixDelegatedAdmin): Verwaltet die Berechtigungen, die Administratoren gewährt werden.
- Citrix Umgebungstestdienst (NT SERVICE\CitrixEnvTest): Verwaltet Selbsttests der anderen Delivery Controller-Dienste.
- Citrix Hostdienst (NT SERVICE\CitrixHostService): Speichert Informationen zu den Hypervisorinfrastrukturen, die in einer XenApp- oder XenDesktop-Bereitstellung verwendet werden, und bietet der Konsole die Funktionalität zum Enumerieren von Ressourcen in einem Hypervisorpool.
- Citrix Maschinenerstellungsdienste (NT SERVICE\CitrixMachineCreationService): Orchestriert das Erstellen von Desktop-VMs.
- Citrix Überwachungsdienst (NT SERVICE\CitrixMonitor): Sammelt Metrik für XenApp oder XenDesktop, speichert historische Informationen und bietet eine Abfrageschnittstelle für Problembehandlungs- und Berichterstattungstools.
- Citrix StoreFront-Dienst (NT SERVICE\CitrixStorefront): Unterstützt die Verwaltung von StoreFront. (Der Dienst selbst gehört nicht zur StoreFront-Komponente.)
- Citrix StoreFront-Dienst für die privilegierte Administration (NT SERVICE\CitrixPrivilegedService): Unterstützt privilegierte Verwaltungsvorgänge von StoreFront. (Der Dienst selbst gehört nicht zur StoreFront-Komponente.)

Bei der Installation des Delivery Controllers werden zudem die folgenden Windows-Dienste erstellt: Diese werden auch erstellt, wenn sie mit anderen Citrix Komponenten installiert werden:

- Citrix Diagnostic Facility COM-Server (NT SERVICE\CdfSvc): Unterstützt das Sammeln von Diagnoseinformationen für den Citrix Support.
- Citrix Telemetriedienst (NT SERVICE\CitrixTelemetryService): Sammelt Diagnoseinformationen zur Analyse durch Citrix. Die Analyseergebnisse und Empfehlungen können von Administratoren angezeigt werden, um die Diagnose von Problemen mit der Site zu erleichtern.

Bei der Installation des Delivery Controllers werden zudem die folgenden Windows-Dienste erstellt: Diese werden zurzeit nicht verwendet und sind deaktiviert. Aktivieren Sie diese Dienste nicht:

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)

Abgesehen vom Citrix StoreFront-Dienst für die privilegierte Administration werden diesen Diensten die Anmeldeberechtigung "Anmelden als Dienst" und die Privilegien "Anpassen von Speicherkontingenten für einen Prozess", "Generieren von Sicherheitsüberwachungen" und "Ersetzen eines Tokens auf Prozessebene" zugewiesen. Sie brauchen die Benutzerrechte nicht zu ändern. Diese Privilegien werden vom Delivery Controller nicht verwendet und werden automatisch deaktiviert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren von Diensteinstellungen

Mit Ausnahme des Citrix StoreFront-Diensts für die privilegierte Administration und des Citrix Telemetriedienst melden sich die oben im Abschnitt Konfigurieren von Benutzerrechten aufgeführten Windows-Dienste des Delivery Controllers als NETWORK SERVICE an. Ändern Sie diese Diensteinstellungen nicht.

Der Citrix StoreFront-Dienst für die privilegierte Administration meldet sich als lokales System an (NT AUTHORITY\SYSTEM). Dies ist für StoreFront-Vorgänge des Delivery Controllers erforderlich, die normalerweise nicht für Dienste verfügbar sind (einschließlich das Erstellen von Microsoft IIS-Sites). Ändern Sie die Diensteinstellungen nicht.

Der Citrix Telemetriedienst meldet sich als seine eigene dienstspezifische Identität an.

Sie können den Citrix Telemetriedienst deaktivieren. Abgesehen von diesem Dienst und Diensten, die bereits deaktiviert sind, deaktivieren Sie keine der anderen Windows-Dienste für Delivery Controller.

# Konfigurieren von Registrierungseinstellungen

Es ist nicht mehr erforderlich, die Erstellung von 8.3-Dateinamen und -Ordnern auf dem VDA-Dateisystem zu aktivieren. Der Registrierungsschlüssel **NtfsDisable8dot3NameCreation** kann zum Deaktivieren der Erstellung von 8.3-Dateinamen und -Ordnern konfiguriert werden. Sie können diese Funktion auch mit dem Befehl **fsutil.exe behavior set disable8dot3** konfigurieren.

# Auswirkungen von Bereitstellungsszenarios auf die Sicherheit

Ihre Benutzerumgebung kann Benutzergeräte enthalten, die von Ihrer Organisation nicht verwaltet werden und dem Vollzugriff der jeweiligen Benutzer unterliegen oder solche, die von Ihrer Organisation verwaltet werden. Die Sicherheitsüberlegungen für diese beiden Umgebungen sind generell unterschiedlich.

**Verwaltete Benutzergeräte**

Verwaltete Benutzergeräte unterliegen einer administrativen Steuerung. Sie werden entweder von Ihnen gesteuert oder von einer anderen Organisation, der Sie vertrauen. Sie können Benutzergeräte konfigurieren und Benutzern direkt bereitstellen. Alternativ können Sie Terminals bereitstellen, auf denen ein einzelner Desktop im Vollbildmodus ausgeführt wird. Befolgen Sie die oben beschriebenen Sicherheitsanweisungen bei allen verwalteten Benutzergeräten. Dieses Release bietet den Vorteil, dass nur ganz wenig Software auf einem Benutzergerät erforderlich ist.

Ein verwaltetes Benutzergerät kann für die Verwendung im Vollbildmodus oder im Fenstermodus konfiguriert werden.

- Im Vollbildmodus können Benutzer sich über den normalen Anmeldebildschirm für Windows anmelden. Dieselben Anmeldeinformationen des Benutzers werden dann zum automatischen Anmelden für dieses Release verwendet.
- Im Fenstermodus melden sich die Benutzer zunächst beim Benutzergerät an. Anschließend melden sie sich über die in diesem Release bereitgestellte Website bei diesem Release an.

**Nicht verwaltete Benutzergeräte**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Benutzergeräte nicht von einer vertrauenswürdigen Organisation verwaltet werden, kann nicht von einer administrativen Steuerung ausgegangen werden. Beispiel: Sie erlauben Benutzern, sich ihre eigenen Geräte zu besorgen und sie zu konfigurieren, doch die Benutzer halten sich u. U. nicht an die oben beschriebenen generellen optimalen Sicherheitsverfahren. Dieses Release hat den Vorteil, nicht verwalteten Benutzergeräten Desktops sicher bereitstellen zu können. Diese Geräte sollten jedoch einen grundlegenden Antivirenschutz haben, um Keylogger und ähnliche Angriffe auf Benutzereingaben abzuwehren.

**Überlegungen zum Datenspeicher**

Mit diesem Release können Sie verhindern, dass Benutzer Daten auf Benutzergeräten speichern, die sie selbst physisch steuern können. Sie müssen dennoch bedenken, welche Auswirkungen es haben kann, wenn Benutzer Daten auf Desktops speichern. Im Allgemeinen sollten Benutzer keine Daten auf Desktops speichern. Daten sollten an einem Ort gespeichert werden, an dem sie entsprechend geschützt werden können, wie z. B. auf Dateiservern, Datenbankservern oder in anderen Repositorys.

Möglicherweise enthält Ihre Desktopumgebung verschiedene Desktoptypen, wie gepoolte und dedizierte Desktops. Benutzer sollten zu keiner Zeit Daten auf Desktops speichern, die für andere Benutzer freigegeben sind, wie z. B. gepoolte Desktops. Wenn Benutzer Daten auf dedizierten Desktops speichern, sollten diese Daten entfernt werden, wenn der Desktop zu einem späteren Zeitpunkt anderen Benutzern zugänglich gemacht wird.

**Umgebungen mit mehreren Versionen**

Umgebungen mit mehreren Versionen sind während einiger Upgrades unvermeidbar. Folgen Sie bewährten Methoden und minimieren Sie die Zeitdauer, während der unterschiedliche Versionen von Citrix Komponenten koexistieren. In Umgebungen mit mehreren Versionen wird beispielsweise die Sicherheitsrichtlinie nicht gleichförmig durchgesetzt.

**Hinweis:** Dies ist typisch für andere Softwareprodukte. Bei Verwendung einer älteren Version von Active Directory wird die Gruppenrichtlinie bei neueren Windows-Versionen nur teilweise durchgesetzt.

Nachfolgend wird eine spezifische Citrix Umgebung mit mehreren Versionen beschrieben, bei der ein Sicherheitsproblem auftreten kann. Wenn Citrix Receiver 1.7 zum Herstellen einer Verbindung mit einem virtuellen Desktop verwendet wird, auf dem der Virtual Delivery Agent in XenApp und XenDesktop 7.6 Feature Pack 2 ausgeführt wird, ist die Richtlinieneinstellung **Dateiübertragungen zwischen Desktop und Client zulassen** für die Site aktiviert, kann jedoch nicht von einem Delivery Controller deaktiviert werden, auf dem XenApp und XenDesktop 7.1 ausgeführt werden. Die Richtlinieneinstellung, die erst in der neueren Version des Produkts hinzugefügt wurde, wird nicht erkannt. Die Richtlinieneinstellung ermöglicht Benutzern das Hochladen und Herunterladen von Dateien zum/vom virtuellen Desktop und repräsentiert damit ein Sicherheitsproblem. Zur Problemumgehung aktualisieren Sie den Delivery Controller bzw. die eigenständige Instanz von Studio auf Version 7.6 Feature Pack 2 und deaktivieren Sie die Richtlinieneinstellung dann mit der Gruppenrichtlinie. Alternativ verwenden Sie die lokale Richtlinie auf allen betroffenen virtuellen Desktops.

# Sicherheitsüberlegungen für Remote-PC-Zugriff

Mit Remote-PC-Zugriff werden die folgenden Sicherheitsfeatures implementiert:

- Die Verwendung von Smartcards wird unterstützt.
- Bei Verbindung einer Remotesitzung wird der Monitor des Büro-PCs leer angezeigt.
- Remote-PC-Zugriff leitet alle Tastatur- und Mauseingaben in die Remotesitzung um, ausgenommen Strg + Alt + Entf, USB-aktivierte Smartcards und biometrische Geräte.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- SmoothRoaming wird nur für einen einzelnen Benutzer unterstützt.
- Wenn ein Benutzer über eine Remotesitzung mit einem Büro-PC verbunden ist, kann nur dieser Benutzer den lokalen Zugriff auf den Büro-PC wiederaufnehmen. Zum Wiederaufnehmen des lokalen Zugriffs muss der Benutzer Strg-Alt-Entf auf dem lokalen PC drücken und sich dann mit denselben Anmeldeinformationen wie für die Remotesitzung anmelden. Er kann zudem auch über eine Smartcard oder biometrische Geräte wieder lokal zugreifen, wenn das System die entsprechende Anmeldeinformationsanbieter-Integration besitzt. Das Standardverhalten kann über die schnelle Benutzerumschaltung über Gruppenrichtlinienobjekte oder durch Bearbeiten der Registrierung außer Kraft gesetzt werden.

**Hinweis:** Citrix empfiehlt, dass Sie VDA-Administratorrechte nicht allgemeinen Sitzungsbenutzern zuweisen.

**Automatische Zuweisungen**

Standardmäßig unterstützt Remote-PC-Zugriff die automatische Zuweisung von mehreren Benutzern zu einem VDA. Unter XenDesktop 5.6 Feature Pack 1 konnten Administratoren dieses Verhalten mit dem PowerShell-Skript RemotePCAccess.ps1 außer Kraft setzen. Dieses Release verwendet einen Registrierungseintrag, mit dem mehrere automatische Remote-PC-Zuweisungen zugelassen oder abgelehnt werden; diese Einstellung gilt für die gesamte Site.

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Beschränken der automatischen Zuweisung auf einen einzelnen Benutzer:

Legen Sie auf jedem Controller in der Site den folgenden Registrierungsschlüssel fest:

> HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer
>
> Name: AllowMultipleRemotePCAssignments
>
> Typ: REG_DWORD
>
> Wert: 0 = Zuweisung mehrerer Benutzer deaktivieren, 1 = (Standard) Zuweisung mehrerer Benutzer aktivieren.

Liegen bereits Benutzerzuweisungen vor, entfernen Sie diese mit SDK-Befehlen, damit der VDA anschließend für eine einzelne automatische Zuweisung zur Verfügung steht.

- Entfernen Sie alle zugewiesenen Benutzer aus dem VDA: $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- Entfernen Sie den VDA aus der Bereitstellungsgruppe: $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

Starten Sie den physischen Büro-PC neu.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Delegierte Administration

Jul 08, 2016

Das Modell der delegierten Administration bietet Flexibilität bei der Delegierung der Administratoraktivitäten mit Rollen und der objektbasierten Steuerung. Die delegierte Administration ist für Bereitstellungen aller Größen geeignet und ermöglicht es Ihnen, mit zunehmender Komplexität der Bereitstellung die Berechtigungsgranularität zu erhöhen. Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche.

- **Administratoren**: Administratoren sind Einzelpersonen oder Personengruppen, die durch ein Active Directory-Konto identifiziert werden. Jeder Administrator ist mit mindestens einem Paar aus Rolle und Geltungsbereich verknüpft.
- **Rollen**: Eine Rolle repräsentiert eine Stellenfunktion und ist mit definierten Berechtigungen ausgestattet. Beispiel: Die Rolle "Bereitstellungsgruppenadministrator" verfügt über Berechtigungen wie etwa "Bereitstellungsgruppe erstellen" und "Desktop aus Bereitstellungsgruppe entfernen". Ein Administrator kann mehrere Rollen für eine Site haben, d. h. eine Person kann sowohl Bereitstellungsgruppenadministrator als auch Maschinenkatalogadministrator sein. Rollen können integriert oder benutzerdefiniert sein.

  Integrierte Rollen:

| Rolle | Berechtigungen |
|---|---|
| Volladministrator | Kann alle Aufgaben und Vorgänge ausführen. Ein Volladministrator wird immer mit dem Geltungsbereich "Alle" kombiniert. |
| Lesezugriffadministrator | Kann alle Objekte in den angegebenen Geltungsbereichen sowie globale Informationen anzeigen, aber nicht ändern. Beispiel: Ein Lesezugriffadministrator mit Geltungsbereich = London kann alle globalen Objekte (z. B. Konfigurationsprotokollierung) und alle London-bezogenen Geltungsbereichsobjekte (z. B. London-Bereitstellungsgruppen) sehen. Dieser Administrator kann jedoch nicht die Objekte im Geltungsbereich "New York" sehen (sofern die Geltungsbereiche "London" und "New York" einander nicht überlappen). |
| Helpdeskadministrator | Kann Bereitstellungsgruppen anzeigen und die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten. Kann den Maschinenkatalog und die Hostinformationen der überwachten Bereitstellungsgruppen sehen sowie Sitzungsverwaltungs- und Energieverwaltungsvorgänge für die Maschinen in diesen Bereitstellungsgruppen durchführen. |
| Maschinenkatalogadministrator | Kann Maschinenkataloge erstellen und verwalten sowie darin Maschinen bereitstellen. Kann Maschinenkataloge aus der Virtualisierungsinfrastruktur, Provisioning Services und von physischen Maschinen anlegen. Mit dieser Rolle können Basisimages verwaltet und Software installiert werden, aber den Benutzern können keine Anwendungen oder Desktops zugewiesen werden. |
| Bereitstellungsgruppenadministrator | Kann Anwendungen, Desktops und Maschinen bereitstellen sowie die mit ihnen verbundenen Sitzungen verwalten. Kann zudem Anwendungs- und Desktopkonfigurationen wie Richtlinien und die Energieverwaltungseinstellungen verwalten. |
| Hostadministrator | Kann Hostverbindungen und ihnen zugeordnete Ressourceneinstellungen verwalten. Kann keine Maschinen, Anwendungen oder Desktops für Benutzer bereitstellen. |

  Bei bestimmten Produkteditionen können Sie benutzerdefinierte Rollen erstellen, um sie den Anforderungen Ihrer Organisation anzupassen und die Berechtigungen entsprechend delegieren. Sie können benutzerdefinierte Rollen dazu verwenden, Berechtigungen in der Granularität einer Aktion oder Aufgabe in einer Konsole zuzuteilen.

- **Geltungsbereiche**: Ein Geltungsbereich steht für eine Sammlung von Objekten. Geltungsbereiche werden verwendet, um die Objekte in einer für Ihre Organisation angemessenen Weise zu gruppieren (z. B. die Bereitstellungsgruppen der Vertriebsabteilung). Objekte können in mehreren Geltungsbereichen vertreten sein, d. h. Objekte können durch einen oder mehrere Geltungsbereiche bezeichnet sein. Der einzige integrierte Geltungsbereich "Alle" enthält alle Objekte. Die Volladministratorrolle bildet immer ein Paar mit dem Geltungsbereich "Alle".

## Beispiel

Firma XYZ entscheidet sich zum Verwalten von Anwendungen und Desktops basierend auf ihrer Abteilungsstruktur (Buchhaltung, Vertrieb und Lager) und ihren Desktopbetriebssystemen (Windows 7 oder Windows 8). Der Administrator erstellt fünf Geltungsbereiche und erfasst jede Bereitstellungsgruppe in zwei Geltungsbereichen: einem Geltungsbereich für die Abteilung, in der sie verwendet werden und einem Geltungsbereich für das verwendete Betriebssystem.

Die folgenden Administratoren wurden erstellt:

| Administrator | Rollen | Geltungsbereiche |
|---|---|---|
| domain/fred | Volladministrator | Alle (Volladministratorrolle wird immer mit "Alle" ausgestattet) |
| domain/rob | Lesezugriffadministrator | Alle |
| domain/heidi | Lesezugriffadministrator<br>Helpdeskadministrator | Alle<br>Vertrieb |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Administrator | Rollen | Geltungsbereiche |
| --- | --- | --- |
| domain/warehouseadmin | Helpdeskadministrator | Lager |
| | | |
| domain/peter | Bereitstellungsgruppenadministrator<br><br>Maschinenkatalogadministrator | Win7 |

- Fred ist Volladministrator und kann alle Elemente im System anzeigen, bearbeiten und löschen.
- Rob kann alle Objekte der Site anzeigen jedoch nicht bearbeiten oder löschen.
- Heidi kann alle Objekte anzeigen und Helpdeskaufgaben an Bereitstellungsgruppen des Geltungsbereichs "Vertrieb" durchführen. Somit kann sie die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten; sie kann allerdings keine Änderungen an der Bereitstellungsgruppe durchführen, wie Hinzufügen oder Entfernen von Maschinen.
- Jedes Mitglied der Active Directory-Sicherheitsgruppe "warehouseadmin" kann Helpdeskaufgaben für Maschinen des Geltungsbereichs "Lager" ausführen.
- Peter ist Spezialist für Windows 7 und kann alle Windows 7-Maschinenkataloge verwalten und Windows 7-Anwendungen, -Desktops und -Maschinen bereitstellen, unabhängig davon, in welchem Abteilungsgeltungsbereich sie sich befinden. Der Administrator erwägt, Peter zum Volladministrator für den Geltungsbereich "Win7" zu machen; entscheidet sich jedoch dagegen, da ein Volladministrator ebenfalls über vollständige Administratorrechte für alle Objekte verfügt, die nicht in einen Geltungsbereich fallen, z. B. "Site" und "Administrator".

### Verwenden der delegierten Administration

Im Allgemeinen hängt die Anzahl der Administratoren und die Granularität der Berechtigungen von der Größe und Komplexität der Bereitstellung ab.

- In kleinen Bereitstellungen oder Testbereitstellungen übernehmen ein oder wenige Administratoren alle Aufgaben und es findet keine Delegierung statt. Erstellen Sie in diesem Fall einen einzelnen Administrator mit der integrierten Rolle "Volladministrator", die den Geltungsbereich "Alle" hat.
- In größeren Bereitstellungen mit mehr Maschinen, Anwendungen und Desktops ist mehr Delegierung erforderlich. Mehrere Administratoren haben möglicherweise bestimmte funktionale Zuständigkeiten (Rollen). Beispiel: Es gibt zwei Volladministratoren, andere sind Helpdeskadministratoren. Weiterhin werden von einem Administrator ggf. nur bestimmte Objektgruppen (Geltungsbereiche) wie Maschinenkataloge verwaltet. Erstellen Sie in diesem Fall neue Geltungsbereiche und Administratoren mit einer der integrierten Rollen und den entsprechenden Geltungsbereichen.
- Noch größere Bereitstellungen erfordern möglicherweise weitere (oder differenziertere) Geltungsbereiche sowie andere Administratoren mit ungewöhnlichen Rollen. Bearbeiten oder erstellen Sie in diesem Fall weitere Geltungsbereiche, erstellen Sie benutzerdefinierte Rollen und erstellen Sie jeden Administrator mit einer integrierten oder benutzerdefinierten Rolle sowie vorhandenen und neuen Geltungsbereichen.

Für mehr Flexibilität und zur Vereinfachung der Konfiguration können Sie neue Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Sie können auch beim Erstellen oder Bearbeiten von Maschinenkatalogen oder Verbindungen Geltungsbereiche festlegen.

### Erstellen und Verwalten von Administratoren

Beim Erstellen einer Site als lokaler Administrator wird dieses Benutzerkonto automatisch zum Volladministrator mit Vollzugriff auf alle Objekte. Nachdem die Site erstellt wurde, verfügen lokale Administratoren über keine besonderen Rechte.

Die Volladministratorrolle hat immer den Geltungsbereich "Alle"; dies kann nicht geändert werden.

Standardmäßig wird ein Administrator aktiviert. Beim Erstellen des neuen Administrators kann das Deaktivieren eines Administrators erforderlich sein, die betroffene Person übernimmt jedoch erst zu einem späteren Zeitpunkt Verwaltungsaufgaben. Bei vorhandenen aktivierten Administratoren kann es vorkommen, dass Sie einige deaktivieren müssen, während Sie Objekte/Geltungsbereiche neu strukturieren und sie dann wieder aktivieren, wenn Sie die Aktualisierung der Konfiguration abgeschlossen haben. Der Volladministrator kann nicht deaktiviert werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist. Das Kontrollkästchen zum Aktivieren/Deaktivieren steht zur Verfügung, wenn Sie einen Administrator erstellen, kopieren oder bearbeiten.

Wenn Sie ein Rollen-/Geltungsbereichspaar beim Kopieren, Bearbeiten oder Löschen eines Administrators löschen, wird nur die Beziehung zwischen Rolle und Geltungsbereich für diesen Administrator gelöscht, jedoch nicht die Rolle oder der Geltungsbereich selbst. Außerdem hat dies keine Auswirkungen auf andere Administratoren, die mit diesem Rollen-/Geltungsbereichspaar konfiguriert sind.

Klicken Sie zum Verwalten von Administratoren im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im mittleren Bereich oben auf die Registerkarte Administratoren.

- Zum Erstellen eines Administrators klicken Sie im Aktionsbereich auf Administrator erstellen. Geben Sie den Namen eines Benutzerkontos ein oder navigieren zu einem Benutzerkonto, wählen oder erstellen Sie einen Geltungsbereich und wählen Sie eine Rolle. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.
- Zum Kopieren eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator kopieren. Geben Sie den Namen des Benutzerkontos ein oder navigieren zu dem Benutzerkonto. Sie können die Rollen-/Geltungsbereichspaare auswählen und dann bearbeiten oder löschen und neue hinzufügen. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.
- Zum Bearbeiten eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator bearbeiten. Sie können die Rollen-/Geltungsbereichspaare bearbeiten oder löschen und neue hinzufügen.
- Zum Löschen eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator löschen. Der Volladministrator kann nicht gelöscht werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist.

### Erstellen und Verwalten von Rollen

Rollennamen können maximal 64 Unicode-Zeichen enthalten. Die folgenden Zeichen sind nicht zulässig: \ (umgekehrter Schrägstrich), / (Schrägstrich), ; (Semikolon), : (Doppelpunkt), # (Nummernzeichen), , (Komma), * (Sternchen), ? (Fragezeichen), = (Gleichheitszeichen) , < (Pfeil nach links), > (Pfeil nach rechts), | (senkrechter Strich), [ ] (eckige Klammern), () (runde Klammern), " (Anführungszeichen) und ' (Apostroph). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Integrierte Rollen können nicht bearbeitet oder gelöscht werden. Benutzerdefinierte Rollen können nicht gelöscht werden, wenn sie von einem Administrator verwendet werden.

Hinweis: Nur bestimmte Produkteditionen unterstützen benutzerdefinierte Rollen. Editionen, die keine benutzerdefinierten Rollen unterstützen, verfügen nicht über verwandte Einträge im Aktionsbereich.
Klicken Sie zum Verwalten von Rollen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im unteren mittleren Bereich auf die Registerkarte Rollen.

- Zum Anzeigen von Rollendetails wählen Sie die Rolle im mittleren Bereich aus. Im unteren Teil des mittleren Bereichs werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie auf die Registerkarte Administratoren im unteren Bereich, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.
- Zum Erstellen einer benutzerdefinierten Rolle klicken Sie im Aktionsbereich auf Rolle erstellen. Geben Sie einen Namen und eine Beschreibung ein. Wählen Sie die Objekttypen und Berechtigungen aus.
- Zum Kopieren einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle kopieren. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Bearbeiten einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Löschen einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle löschen. Bestätigen Sie die Löschung.

### Erstellen und Verwalten von Geltungsbereichen

Beim Erstellen einer Site steht nur der Geltungsbereich "Alle" zur Verfügung. Dieser kann nicht gelöscht werden.

Sie können Geltungsbereiche mit der unten aufgeführten Vorgehensweise erstellen. Sie können auch die Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Jeder Administrator muss mindestens einem Rollen-/Geltungsbereichspaar zugeordnet werden. Beim Erstellen oder Bearbeiten von Desktops, Maschinenkatalogen, Anwendungen oder Hosts können Sie diese einem bestehenden Geltungsbereich hinzufügen. Wenn Sie sie keinem Geltungsbereich hinzufügen, bleiben sie Teil des Geltungsbereichs "Alle".

Die Geltungsbereichszuordnung ist bei der Erstellung von Sites und für Objekte der delegierten Administration (Geltungsbereiche und Rollen) nicht möglich. Objekte, die nicht zugeordnet werden können, gehören zum Geltungsbereich "Alle". (Volladministratoren ist immer der Geltungsbereich "Alle" zugeordnet.) Maschinen, Energieaktionen, Desktops und Sitzungen werden nicht direkt einem Geltungsbereich zugeordnet. Administratoren können Berechtigungen für diese Objekte über die zugehörigen Maschinenkataloge oder Bereitstellungsgruppen zugewiesen werden.

Geltungsbereichsnamen können maximal 64 Unicode-Zeichen enthalten. Die folgenden Zeichen sind nicht zulässig: \ (umgekehrter Schrägstrich), / (Schrägstrich), ; (Semikolon), : (Doppelpunkt), # (Nummernzeichen), , (Komma), * (Sternchen), ? (Fragezeichen), = (Gleichheitszeichen) , < (Pfeil nach links), > (Pfeil nach rechts), | (senkrechter Strich), [ ] (eckige Klammern), () (runde Klammern), " (Anführungszeichen) und ' (Apostroph). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.

Wenn Sie einen Geltungsbereich kopieren oder bearbeiten, dürfen Sie nicht vergessen, dass Objekte, die aus dem Geltungsbereich entfernt werden, für den Administrator ggf. nicht mehr zugänglich sind. Ist der bearbeitete Geltungsbereich mit einer oder mehreren Rollen gepaart, stellen Sie sicher, dass durch Änderungen an dem Bereich kein Rollen-/Geltungsbereichspaar unbrauchbar wird.

Klicken Sie zum Verwalten von Geltungsbereichen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im mittleren Bereich oben auf die Registerkarte Geltungsbereiche.

- Zum Erstellen eines Geltungsbereichs klicken Sie im Aktionsbereich auf Geltungsbereich erstellen. Geben Sie einen Namen und eine Beschreibung ein. Zum Einschließen aller Objekte eines bestimmten Typs (z. B. Bereitstellungsgruppen), wählen Sie den Objekttyp aus. Zum Einschließen bestimmter Objekte erweitern Sie den Typ und wählen Sie die einzelnen Objekte (z. B. einzelne Bereitstellungsgruppen des Vertriebs) aus.
- Zum Kopieren eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich kopieren. Geben Sie einen Namen und eine Beschreibung ein. Ändern Sie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Bearbeiten eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf.
- Zum Löschen eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich löschen. Bestätigen Sie die Löschung.

### Erstellen von Berichten

Sie können zwei Arten delegierter Administrationsberichte erstellen:

- Einen HTML-Bericht, der die Rollen-/Geltungsbereichspaare, die einem Administrator zugeordnet sind, sowie die einzelnen Berechtigungen für jeden Objekttyp (z. B. Bereitstellungsgruppen, und Maschinenkataloge) enthält. Sie generieren diesen Bericht in Studio.
  Zum Erstellen dieses Berichts klicken Sie im Navigationsbereich auf Konfiguration > Administratoren. Wählen Sie im mittleren Bereich einen Administrator aus, und klicken Sie dann im Aktionsbereich auf Bericht erstellen.

  Sie können diesen Bericht auch beim Erstellen, Kopieren oder Bearbeiten eines Administrators anfordern.

- HTML- oder CSV Bericht, in dem alle integrierten benutzerdefinierten Rollen und Berechtigungen zugeordnet sind. Sie generieren diesen Bericht durch Ausführen des PowerShell-Skripts "OutputPermissionMapping.ps1".
  Um dieses Skript auszuführen, müssen Sie ein Volladministrator, ein Lesezugriffadministrator oder ein benutzerdefinierter Administrator mit der Berechtigung zum Lesen von Rollen sein. Das Skript befindet sich in: Programme\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

  Syntax:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

| Parameter | Beschreibung |
|---|---|
| -Help | Zeigt Skripthilfe an. |
| -Csv | Gibt CSV-Ausgabe an. Standard = HTML |
| -Path | Zielspeicherort für die Ausgabe. Standard = stdout |
| -AdminAddress | IP-Adresse oder Hostname des Delivery Controllers, mit dem eine Verbindung hergestellt wird. Standard = localhost |
| -Show | Gilt nur, wenn der Parameter "-Path" ebenfalls angegeben wird. Wenn die Ausgabe in eine Datei geschrieben wird, wird sie mit -Show in einem geeigneten Programm, z. B. einem Webbrowser, geöffnet. |
| | Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer und OutVariable. Weitere Informationen finden Sie in der Dokumentation von Microsoft. |

Mit dem Befehl im folgenden Beispiel wird eine HTML-Tabelle in eine Datei namens Roles.html geschrieben und die Tabelle in einem Webbrowser geöffnet.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  -Path Roles.html –Show
```

Mit dem Befehl im folgenden Beispiel wird eine CSV-Tabelle in eine Datei namens Roles.csv geschrieben. Die Tabelle wird nicht angezeigt.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  –CSV -Path Roles.csv
```

An einer Windows-Eingabeaufforderung wird der Befehl aus dem vorherigen Beispiel folgendermaßen eingegeben:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'  -CSV -Path Roles.csv"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Smartcards

Aug 17, 2016

Smartcards und ähnliche Technologien werden im Rahmen der folgenden Vorgaben unterstützt. Folgendes gilt für die Verwendung von Smartcards mit XenApp oder XenDesktop:

- Machen Sie sich mit den Sicherheitsrichtlinien Ihrer Organisation für die Verwendung von Smartcards vertraut. Mit diesen Richtlinien wird z. B. festgelegt, wie Smartcards ausgegeben werden und wie diese von Benutzern gesichert werden sollten. Einige Aspekte dieser Richtlinien müssen ggf. in einer XenApp- bzw. XenDesktop-Umgebung neu bewertet werden.
- Legen Sie fest, welche Benutzergerätetypen, Betriebssysteme und veröffentlichten Anwendungen mit Smartcards verwendet werden dürfen.
- Machen Sie sich mit der Smartcard-Technologie und der Hardware und Software des von Ihnen gewählten Smartcardanbieters vertraut.
- Sie sollten wissen, wie Sie digitale Zertifikate in einer verteilten Umgebung bereitstellen.

# Smartcardtypen

Smartcards für Unternehmen und Kunden haben die gleiche Größe, elektrischen Verbindungen und passen in die gleichen Smartcardleser.

Smartcards für Unternehmen enthalten digitale Zertifikate. Diese Smartcards unterstützen die Windows-Anmeldung und können auch mit Anwendungen für digitale Signaturen und die Verschlüsselung von Dokumenten und E-Mail verwendet werden. Diese Verwendungsmöglichkeiten werden von XenApp und XenDesktop unterstützt.

Smartcards für Kunden enthalten keine digitalen Zertifikate, sondern einen gemeinsamen geheimen Schlüssel. Diese Smartcards können Zahlungen unterstützen (z. B. eine Kreditkarte mit Chip und Unterschrift oder Chip und PIN). Sie bieten keine Unterstützung für Windows-Anmeldung oder typische Windows-Anwendungen. Für die Verwendung dieser Smartcards sind spezielle Windows-Anwendungen und eine geeignete Software-Infrastruktur (einschließlich einer Verbindung zu einem Zahlungskartennetzwerk) erforderlich. Informationen zur Unterstützung dieser speziellen Anwendungen auf XenApp oder XenDesktop erhalten Sie von einem Citrix Mitarbeiter.

Für Unternehmenssmartcards gibt es entsprechende kompatible Technologien, die ähnlich funktionieren.

- Ein smartcardäquivalentes USB-Token stellt eine direkte Verbindung mit einem USB-Anschluss her. Diese USB-Token sind normalerweise so groß wie ein USB-Stick, aber sie können auch so klein wie die SIM-Karte eines Mobiltelefons sein. Sie sind eine Kombination aus einer Smartcard und einem USB-Smartcardleser.
- Eine virtuelle Smartcard, die ein Windows Trusted Platform Module (TPM) verwendet, wird als Smartcard angezeigt. Diese virtuellen Smartcards werden für Windows 8 und Windows 10 mit Citrix Receiver ab Version 4.3 unterstützt.
  - XenApp- und XenDesktop-Versionen vor Version 7.6 FP3 unterstützen keine virtuellen Smartcards.
  - Weitere Informationen zu virtuellen Smartcards finden Sie unter Virtual Smart Card Overview.

> **Hinweis:** Der Begriff "virtuelle Smartcard" wird auch für ein digitales Zertifikat verwendet, das auf dem Computer des Benutzers gespeichert wird. Diese digitalen Zertifikate sind nicht unbedingt gleichbedeutend mit Smartcards.

Die Smartcard-Unterstützung in XenApp und XenDesktop basiert auf dem PC/SC-Standard (Personal Computer/Smart Card) von Microsoft. Als Mindestanforderung müssen Smartcards und Smartcardleser vom zugrunde liegenden Windows-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Betriebssystem unterstützt werden und vom Microsoft Windows Hardware Quality Labs (WHQL) für die Verwendung auf Computern mit einem qualifizierenden Windows-Betriebssystem zugelassen sein. Weitere Informationen zur PC/SC-Kompatibilität von Hardware finden Sie in der Microsoft Dokumentation. Auch andere Benutzergeräte entsprechen möglicherweise dem PS/SC-Standard. Weitere Informationen finden Sie auf der Website des Citrix Ready-Programms unter http://www.citrix.com/ready/.

Normalerweise sind für die Smartcards der unterschiedlichen Anbieter oder für ähnliche Lösungen separate Gerätetreiber erforderlich. Wenn Smartcards jedoch einem Standard wie dem NIST Personal Identity Verification (PIV)-Standard entsprechen, kann möglicherweise ein Gerätetreiber für eine Reihe von Smartcards verwendet werden. Der Gerätetreiber muss auf dem Benutzergerät und dem Virtual Delivery Agent (VDA) installiert werden. Der Gerätetreiber wird häufig von einem Citrix Partner im Rahmen eines Smartcard-Middleware-Pakets zur Verfügung gestellt, das erweiterte Features bietet. Der Gerätetreiber wird u. U. auch Kryptografiedienstanbieter (Cryptographic Service Provider, CSP), Schlüsselspeicheranbieter (Key Storage Provider, KSP) oder Minitreiber genannt.

Die folgenden Kombinationen aus Smartcard und Middleware für Windows-Systeme wurden von Citrix als repräsentatives Beispiel ihres Typs getestet. Es können jedoch auch andere Smartcards und Middleware verwendet werden. Weitere Informationen über Citrix-kompatible Smartcards und Middleware finden Sie unter http://www.citrix.com/ready.

| Middleware | Geeignete Karten |
|---|---|
| ActivClient 7.0 (DoD-Modus aktiviert) | DoD CAC-Karte |
| ActivClient 7.0 im PIV-Modus | NIST PIV-Karte |
| Microsoft-Minitreiber | NIST PIV-Karte |
| Gemalto-Minitreiber für .NET-Karte | Gemalto .NET v2+ |
| nativer Microsoft-Treiber | virtuelle Smartcards (TPM) |

Informationen zur Verwendung von Smartcards mit anderen Gerätetypen finden Sie in der Citrix Receiver-Dokumentation für das Gerät. Weitere Informationen zur Verwendung von PIV mit XenDesktop finden Sie unter Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV SmartCard Authentication.

Informationen zur Verwendung von Smartcards mit anderen Gerätetypen finden Sie in der Citrix Receiver-Dokumentation für das jeweilige Gerät.

### Remote-PC-Zugriff

Smartcards werden nur für den Remotezugriff auf physische Büro-PCs mit Windows 10, Windows 8 oder Windows 7 unterstützt; Smartcards werden nicht für Büro-PCs mit Windows XP unterstützt.

Die folgenden Smartcards wurden mit Remote-PC-Zugriff getestet:

| Middleware | Geeignete Karten |
|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Gemalto .NET-Minitreiber | Gemalto .NET v2+ |
| ActivIdentity ActivClient 6.2 | NIST PIV |
| ActivIdentity ActivClient 6.2 | CAC |
| Microsoft-Minitreiber | NIST PIV |
| nativer Microsoft-Treiber | Virtuelle Smartcards |

# Smartcardleser

Ein Smartcardleser kann in das Benutzergerät integriert sein oder extern an das Benutzergerät angeschlossen werden (normalerweise über USB oder Bluetooth). Kontaktbehaftete Kartenleser, die USB-CCID-konform (Chip/Smart Card Interface Devices) sind, werden unterstützt. Diese enthalten einen Schlitz, in den die Smartcard eingeführt wird. Kontaktbehaftete Kartenleser werden gemäß einer DK-Spezifikation (Deutsche Kreditwirtschaft) in vier Klassen eingeteilt.

- Smartcardleser der Klasse 1 sind die häufigsten Geräte und haben normalerweise nur einen Steckplatz. Smartcardleser der Klasse 1 werden in der Regel durch einen CCID-Standardgerätetreiber unterstützt, der mit dem Betriebssystem geliefert wurde.
- Smartcardleser der Klasse 2 verfügen über eine sichere Tastatur, auf die über das Benutzergerät nicht zugegriffen werden kann. Diese Smartcardleser können auch in eine Tastatur integriert sein. Wenn Sie Smartcardleser der Klasse 2 verwenden, wenden Sie sich an einen Citrix Mitarbeiter, da u. U. ein spezifischer Gerätetreiber erforderlich ist, damit die sichere Tastatur funktioniert.
- Smartcardleser der Klasse 3 haben ein sicheres Display. Sie werden nicht unterstützt.
- Smartcardleser der Klasse 4 haben ein sicheres Übertragungsmodul. Diese Smartcardleser werden nicht unterstützt.

**Hinweis:** Die Klasse der Smartcardleser hat nichts mit der USB-Geräteklasse zu tun.

Smartcardleser müssen mit einem entsprechenden Gerätetreiber auf dem Benutzergerät installiert sein.

# Benutzererfahrung

Smartcardunterstützung ist in XenApp und XenDesktop durch einen bestimmten virtuellen ICA/HDX-Smartcardkanal integriert, der standardmäßig aktiviert ist.

**Wichtig:** Verwenden Sie für Smartcardleser keine generische USB-Umleitung. Sie ist für Smartcardleser standardmäßig deaktiviert und wird auch bei Aktivierung nicht unterstützt.

Auf einem Benutzergerät können mehrere Smartcards und mehrere Smartcardleser verwendet werden. Wenn Passthrough-Authentifizierung verwendet wird, darf jedoch nur eine Smartcard eingelegt sein, wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet. Wenn eine Smartcard in einer Anwendung verwendet wird (z. B. zum digitalen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Signieren oder für Verschlüsselungsfunktionen), werden möglicherweise zusätzliche Aufforderungen zum Einführen einer Smartcard oder zum Eingeben einer PIN angezeigt. Dies kann auftreten, wenn mehr als eine Smartcard eingelegt wurde.

- Wenn Benutzer zum Einlegen einer Smartcard aufgefordert werden und diese sich bereits im Leser befindet, sollten sie auf "Abbrechen" klicken.
- Wenn Benutzer zur Eingabe der PIN-Nummer aufgefordert werden, sollten sie diese erneut eingeben.

Wenn Sie gehostete Anwendungen unter Windows Server 2008 oder 2008 R2 und mit Smartcards verwenden, die den Microsoft-Kryptografiedienstanbieter für Basissmartcards benötigen, werden im Fall der Ausführung einer Smartcard-Transaktion alle anderen Benutzer, die eine Smartcard bei der Anmeldung verwendet haben, blockiert. Weitere Details und einen Hotfix zur Behebung dieses Problems finden Sie unter http://support.microsoft.com/kb/949538.

Sie können PINs mit einem Kartenverwaltungsprogramm oder einem Herstellerdienstprogramm zurücksetzen.

# Führen Sie vor dem Bereitstellen von Smartcards folgende Schritte aus:

- Installieren Sie für den Smartcardleser einen Gerätetreiber auf dem Benutzergerät. Viele Smartcardleser können mit dem von Microsoft bereitgestellten CCID-Gerätetreiber benutzt werden.
- Beziehen Sie einen Gerätetreiber und Kryptografiedienstanbietersoftware (CSP) vom Smartcard-Hersteller und installieren Sie beides auf Benutzergeräten und auf virtuellen Desktops. Der Treiber und die CSP-Software müssen mit XenApp bzw. XenDesktop kompatibel sein (Informationen zur Kompatibilität enthält die Dokumentation). Für virtuelle Desktops mit Smartcards, die das Minitreibermodell unterstützen und verwenden, werden die Smartcard-Minitreiber automatisch heruntergeladen. Die Treiber können auch über http://catalog.update.microsoft.com oder den Hersteller bezogen werden. Wird PKCS#11-Middleware benötigt, wenden Sie sich an den Smartcardhersteller.
- **Wichtig**: Citrix empfiehlt, dass Sie die Treiber und CSP-Software vor der Installation von Citrix Software auf einem physischen Computer installieren und testen.
- Fügen Sie die Citrix Receiver für Web-URL der Liste der vertrauenswürdigen Sites für Benutzer hinzu, die mit Smartcards im Internet Explorer unter Windows 10 arbeiten. In Windows 10 wird Internet Explorer für vertrauenswürdige Sites nicht standardmäßig im geschützten Modus ausgeführt.
- Stellen Sie sicher, dass die Public Key-Infrastruktur entsprechend konfiguriert ist. Hierzu gehört, dass die Zertifikat-zu-Konto-Zuordnung richtig für die Active Directory-Umgebung konfiguriert ist, und dass die Validierung des Benutzerzertifikats ausgeführt werden kann.
- Stellen Sie sicher, dass die Bereitstellung die Systemanforderungen der anderen Citrix Komponenten erfüllt, die mit Smartcards verwendet werden, u. a. Citrix Receiver und StoreFront.
- Stellen Sie sicher, dass auf die folgenden Server in der Site Zugriff besteht:
  - Active Directory-Domänencontroller für das Benutzerkonto mit zugeordnetem Anmeldezertifikat auf der Smartcard
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional für Remotezugriff): Microsoft Exchange Server

# Aktivieren der Smartcard-Verwendung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Schritt 1:** Geben Sie die Smartcards an die Benutzer aus und berücksichtigen Sie dabei die Kartenausstellungsrichtlinie.

**Schritt 2:** (Optional): Richten Sie Smartcards ein, damit Benutzer Remote-PC-Zugriff verwenden können.

**Schritt 3:** Installieren Sie ggf. den Delivery Controller und StoreFront und konfigurieren Sie beides für Smartcard-Remoting.

**Schritt 4:** Aktivieren Sie StoreFront für die Verwendung mit Smartcards. Einzelheiten finden Sie unter "Konfigurieren der Smartcardauthentifizierung" in der StoreFront-Dokumentation.

**Schritt 5:** Aktivieren Sie NetScaler Gateway/Access Gateway für die Verwendung mit Smartcards. Einzelheiten finden Sie unter "Configuring Authentication and Authorization" und "Configuring Smart Card Access with the Web Interface" in der NetScaler-Dokumentation.

**Schritt 6:** Aktivieren Sie VDAs für die Verwendung mit Smartcard.

- Stellen Sie sicher, dass die erforderlichen Anwendungen und Updates auf dem VDA installiert wurden.
- Installieren Sie die Middleware.
- Richten Sie Smartcard-Remoting ein, damit die Kommunikation von Smartcarddaten zwischen Citrix Receiver auf einem Benutzergerät und einer virtuellen Desktopsitzung möglich ist.

**Schritt 7:** Aktivieren Sie Benutzergeräte (einschließlich der Maschinen innerhalb und außerhalb von Domänen) für die Verwendung von Smartcards. Einzelheiten finden Sie unter "Konfigurieren der Smartcardauthentifizierung" in der StoreFront-Dokumentation.

- Importieren Sie das Zertifizierungsstellen-Stammzertifikat und das Zertifikat der ausstellenden Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
- Installieren Sie die Smartcard-Middleware des Herstellers.
- Installieren und konfigurieren Sie Citrix Receiver für Windows. Stellen Sie sicher, dass Sie icaclient.adm mit der Gruppenrichtlinien-Verwaltungskonsole importieren und die Smartcard-Authentifizierung aktivieren.

**Schritt 8:** Testen Sie die Bereitstellung. Stellen Sie sicher, dass die Bereitstellung richtig konfiguriert ist, indem Sie den virtuellen Desktop mit der Smartcard eines Testbenutzers starten. Testen Sie alle möglichen Zugriffsmechanismen (beispielsweise Zugriff auf den Desktop über Internet Explorer und Citrix Receiver).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Smartcardbereitstellungen

Jul 08, 2016

Die folgenden Typen von Smartcardbereitstellungen werden von dieser Produktversion und von gemischten Umgebungen, die diese Version enthalten, unterstützt. Weitere Konfigurationen funktionieren eventuell, werden aber nicht unterstützt.

| Eingabe | Verbindung mit StoreFront |
|---|---|
| Lokale in Domänen eingebundene Computer | Direkte Verbindung |
| Remotezugriff von in Domänen eingebundenen Computern | Verbindung über NetScaler Gateway |
| Nicht in Domänen eingebundene Computer | Direkte Verbindung |
| Remotezugriff von nicht in Domänen eingebundenen Computern | Verbindung über NetScaler Gateway |
| Nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite | Verbindung über Desktopgerätesites |
| In Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL | Verbindung über XenApp Services-URLs |

Die Bereitstellungstypen werden durch die Merkmale des Benutzergeräts definiert, mit dem der Smartcardleser verbunden ist:

- In Domäne eingebundenes Gerät oder nicht in Domäne eingebundenes Gerät
- Art der Verbindung zwischen Gerät und StoreFront
- Zur Anzeige der virtuellen Desktops und Anwendungen verwendete Software

Darüber hinaus können smartcardfähige Anwendungen wie Microsoft Word oder Microsoft Excel in diesen Bereitstellungen verwendet werden. In diesen Anwendungen können Benutzer Dokumente digital signieren und verschlüsseln.

## Bimodale Authentifizierung

Soweit in der jeweiligen Bereitstellung möglich, unterstützt Receiver die bimodale Authentifizierung, d. h. der Benutzer hat die Wahl, sich mit einer Smartcard oder mit dem Benutzernamen und Kennwort anzumelden. Dies ist nützlich, wenn die Smartcard nicht verwendet werden kann (z. B. sie wurde vom Benutzer zu Hause vergessen oder das Zertifikat ist abgelaufen).

Da Benutzer nicht domänengebundener Geräte sich direkt an Receiver für Windows anmelden, können Sie für diese Benutzer ein Fallback auf die explizite Authentifizierung aktivieren. Wenn Sie die bimodale Authentifizierung konfigurieren, müssen sich Benutzer zuerst mit den Smartcards und PINs anmelden; sie können aber die explizite Authentifizierung auswählen, wenn sie Probleme mit den Smartcards haben.

Wenn Sie NetScaler Gateway bereitstellen, melden sich Benutzer an den Geräten an und werden von Receiver für Windows zur Authentifizierung bei NetScaler Gateway aufgefordert. Dies gilt sowohl für in Domänen eingebundene Geräte als auch


© 1999-2017 Citrix Systems, Inc. All rights reserved.

für Geräte, die nicht in Domänen eingebunden sind. Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie können dann Benutzern die bimodale Authentifizierung für Anmeldungen an NetScaler Gateway bereitstellen. Konfigurieren Sie die Passthrough-Authentifizierung von NetScaler Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an NetScaler Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden.

### Überlegungen zu mehreren Active Directory-Gesamtstrukturen

In einer Citrix Umgebung werden Smartcards in einer einzelnen Gesamtstruktur unterstützt. Strukturübergreifende Smartcard-Anmeldungen erfordern eine direkte bidirektionale Gesamtstruktur-Vertrauensstellung für alle Benutzerkonten. Komplexere Mehrfachstruktur-Bereitstellungen mit Smartcards (d. h. Vertrauensstellungen sind nur unidirektional oder sonstiger Art) werden nicht unterstützt.

Sie können Smartcards in einer Citrix Umgebung mit Remotedesktops verwenden. Dieses Feature kann lokal installiert werden (auf dem Benutzergerät, mit dem die Smartcard verbunden ist) oder remote (auf dem Remotedesktop, mit dem das Benutzergerät verbunden wird).

### Richtlinie zum Entfernen der Smartcard

Die Richtlinie zum Entfernen der Smartcard legt fest, was passiert, wenn die Smartcard während einer Sitzung entfernt wird. Die Richtlinie zum Entfernen der Smartcard wird im Windows-Betriebssystem konfiguriert und verarbeitet.

| Richtlinieneinstellung | Desktop-Verhalten |
|---|---|
| Keine Aktion | Keine Aktion. |
| Arbeitsstation sperren | Die Desktopsitzung wird getrennt und der virtuelle Desktop gesperrt. |
| Abmeldung erzwingen | Der Benutzer wird zur Abmeldung gezwungen. Wenn die Netzwerkverbindung unterbrochen ist und diese Einstellung aktiviert wird, wird die Sitzung möglicherweise abgemeldet und der Benutzer verliert Daten. |
| Trennen bei einer Remotedienstesitzung | Die Sitzung wird getrennt und der virtuelle Desktop gesperrt. |

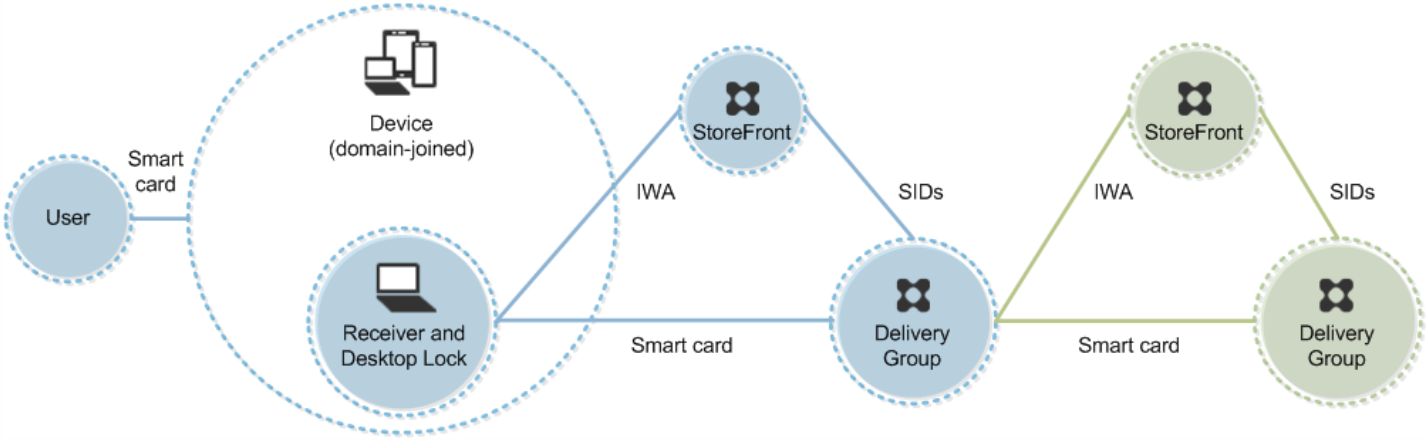
### Überprüfen der Zertifikatsperrlisten

Wenn die Überprüfung von Zertifikatsperrlisten aktiviert ist und ein Benutzer führt eine Smartcard mit einem ungültigen Zertifikat in einen Smartcardleser ein, kann der Benutzer nicht authentifiziert werden oder nicht auf den mit dem Zertifikat verbundenen Desktop oder die Anwendung zugreifen. Bei einem ungültigen Zertifikat für die E-Mail-Entschlüsselung bleibt die E-Mail beispielsweise verschlüsselt. Wenn andere Zertifikate auf der Smartcard, z. B. solche, die für die Authentifizierung verwendet werden, noch gültig sind, bleiben diese Funktionen weiterhin aktiv.

### Bereitstellungsbeispiel: in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

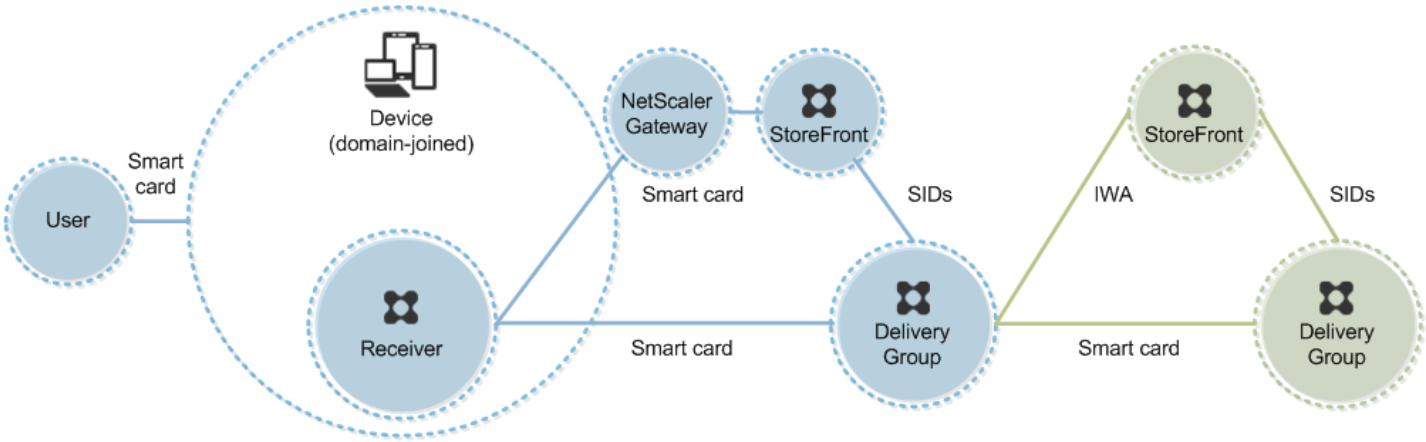



Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Der Benutzer wird dann durch Receiver beim Storefront-Server mittels integrierter Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On" konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### Bereitstellungsbeispiel: Remotezugriff von in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Verbindung mit StoreFront über NetScaler Gateway/Access Gateway.




Der Benutzer meldet sich mit Smartcard und PIN beim Gerät und anschließend erneut bei NetScaler Gateway oder Access Gateway an. Die zweite Anmeldung kann entweder mit Smartcard und PIN oder einem Benutzernamen und einem Kennwort erfolgen, da Receiver in dieser Bereitstellung eine bimodale Authentifizierung zulässt.

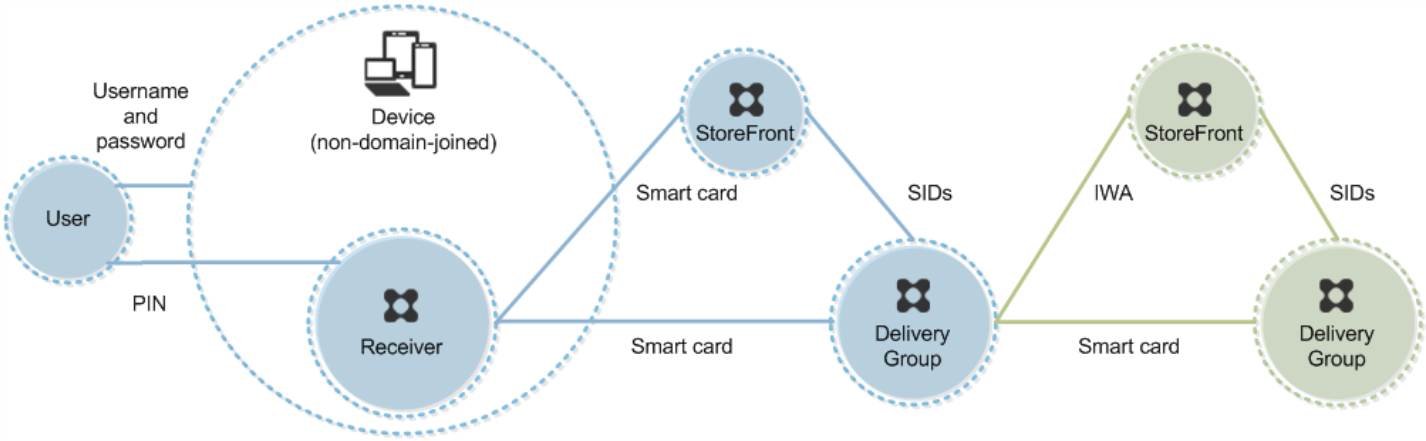
Der Benutzer wird automatisch bei StoreFront angemeldet; StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On" konfiguriert ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.




Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

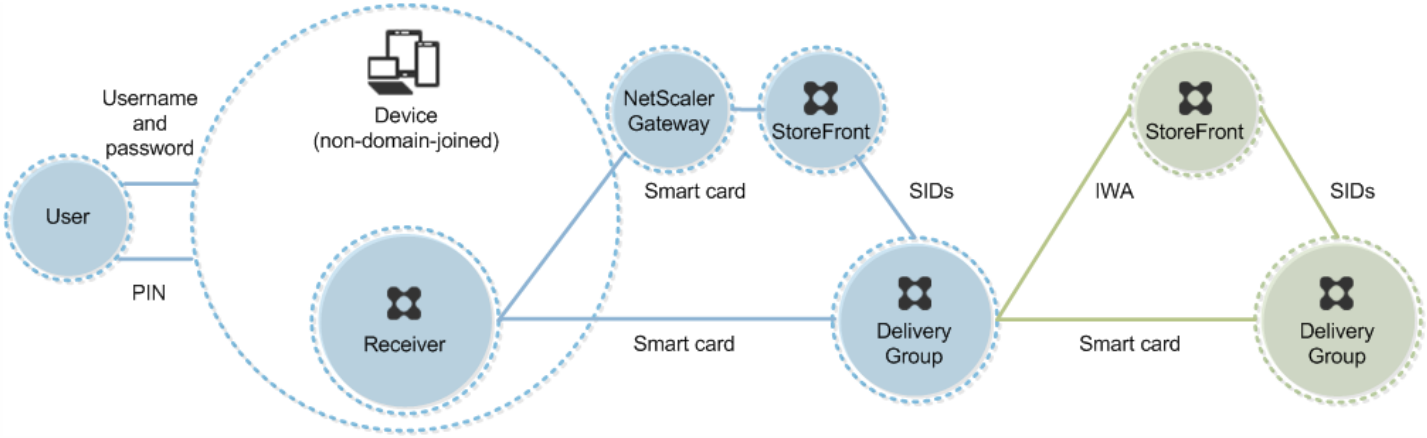
StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### Bereitstellungsbeispiel: Remotezugriff von nicht in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

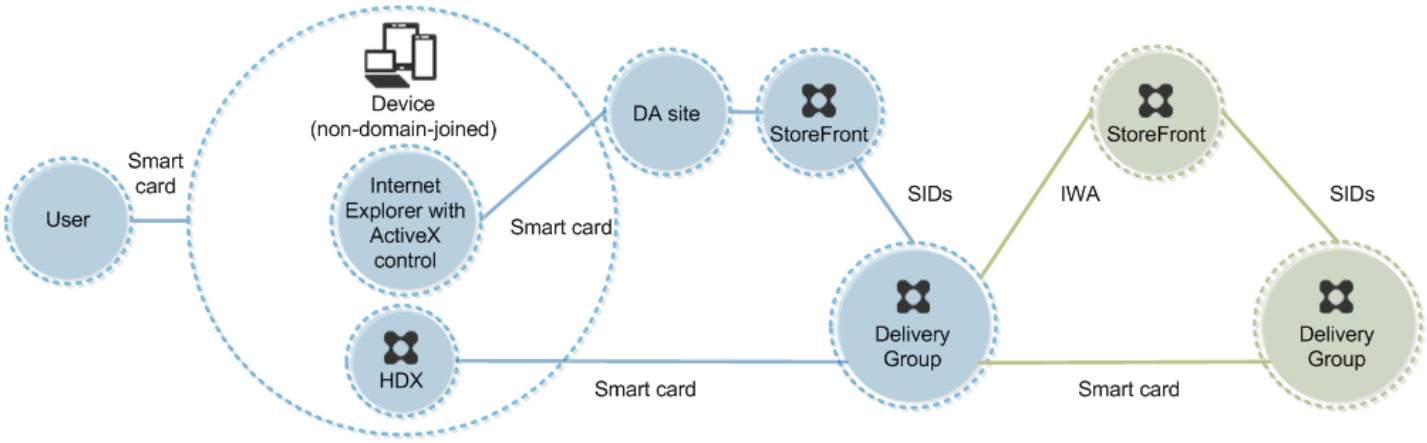
Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte, auf denen möglicherweise Desktop Lock ausgeführt wird und die mit StoreFront über Desktopgerätesites verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird das Gerät so konfiguriert, dass eine Desktopgerätesite über Internet Explorer im Kioskmodus gestartet wird. Der Benutzer wird durch ein ActiveX-Steuerelement der Site aufgefordert, seine PIN einzugeben, die dann an StoreFront gesendet wird. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Der erste verfügbare Desktop in der alphabetischen Liste einer zugewiesenen Desktopgruppe wird gestartet.

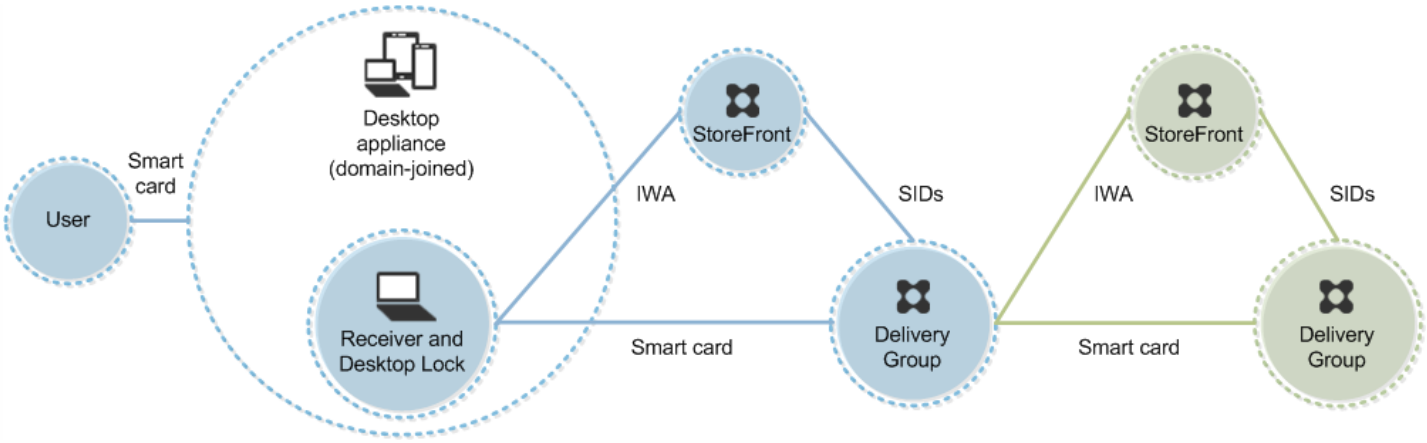
Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### Bereitstellungsbeispiel: in Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte, auf denen Desktop Lock ausgeführt wird und die mit StoreFront über XenApp Services-URLs verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird der Benutzer beim Storefront-Server über die integrierte Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver Single Sign-On konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Passthrough-Authentifizierung und Single Sign-On mit Smartcards

Jul 08, 2016

## Passthrough-Authentifizierung

Die Passthrough-Authentifizierung mit Smartcards bei virtuellen Desktops wird auf Benutzergeräten unterstützt, auf denen Windows 10, Windows 8 und Windows 7 SP1, Enterprise und Professional Editionen ausgeführt werden.

Die Passthrough-Authentifizierung mit Smartcards bei gehosteten Anwendungen wird auf Servern unterstützt, auf denen Windows Server 2008 und Windows Server 2012 ausgeführt werden.

Wenn Sie die Passthrough-Authentifizierung mit Smartcards für gehostete Anwendungen verwenden, stellen Sie sicher, dass Sie für Passthrough mit Smartcard als Authentifizierungsmethode für die Site die Verwendung von Kerberos aktivieren.

Hinweis: Die Verfügbarkeit der Passthrough-Authentifizierung mit Smartcards hängt von vielen Faktoren ab, u. a.:

- Sicherheitsrichtlinien für die Passthrough-Authentifizierung der jeweiligen Organisation
- Typ und Konfiguration der Middleware
- Typen der Smartcardleser
- Richtlinie für das Zwischenspeichern von Middleware-PINs

Die Passthrough-Authentifizierung mit Smartcards wird in Citrix StoreFront konfiguriert. Weitere Informationen finden Sie unter
*— Konfigurieren des Authentifizierungsdiensts*
in der StoreFront-Dokumentation.

## Single Sign-On

Single Sign-On ist ein Citrix Feature, mit dem die Passthrough-Authentifizierung in Starts von virtuellen Desktops und Anwendungen implementiert wird. Sie können dieses Feature bei Smartcardbereitstellungen verwenden, die in Domänen eingebunden und direkt mit StoreFront verbunden sind, sowie bei in Domänen eingebundenen und über NetScaler mit StoreFront verbundenen Bereitstellungen. So müssen Benutzer ihre PIN weniger häufig eingeben. Zur die Verwendung von Single Sign-On in diesen Bereitstellungstypen bearbeiten Sie die folgenden Parameter in der Datei default.ica, die sich auf dem StoreFront-Server befindet:

- In Domänen eingebundene, direkt mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für DisableCtrlAltDel auf Off
- In Domänen eingebundene, über NetScaler mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für UseLocalUserAndPassword auf On

Weitere Anweisungen zum Einrichten dieser Parameter finden Sie in der Dokumentation für StoreFront oder NetScaler Gateway.

Die Verfügbarkeit der Single Sign-On-Funktion hängt von vielen Faktoren ab, u. a.:

- Sicherheitsrichtlinien für Single Sign-On der jeweiligen Organisation
- Typ und Konfiguration der Middleware
- Typen der Smartcardleser
- Richtlinie für das Zwischenspeichern von Middleware-PINs


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Wenn Benutzer sich beim Virtual Delivery Agent (VDA) mit einer Maschine anmelden, an die ein Smartcardleser angeschlossen ist, wird möglicherweise eine Windows-Kachel angezeigt, die die letzte erfolgreiche Authentifizierungsmethode repräsentiert, z. B. Smartcard oder Kennwort. Daher wird bei aktiviertem Single Sign-On ggf. eine entsprechende Kachel angezeigt. Zum Anmelden müssen Benutzer Benutzer wechseln auswählen, um eine andere Kachel auszuwählen, da die Single Sign-On-Kachel nicht funktioniert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Transport Layer Security (TLS)

Aug 17, 2016

Das Konfigurieren einer XenApp- oder XenDesktop-Site zur Verwendung des TLS-Sicherheitsprotokolls (Transport Layer Security) umfasst folgende Schritte:

- Rufen Sie ein Serverzertifikat ab und installieren und registrieren Sie es auf allen Delivery Controllern. Konfigurieren Sie zudem einen Port mit dem SSL-Zertifikat. Einzelheiten finden Sie unter Installieren von TLS-Serverzertifikaten auf Controllern.
  Sie können die Ports ändern, die der Controller zum Abhören von HTTP- und HTTPS-Datenverkehr verwendet.

- Aktivieren Sie TLS-Verbindungen zwischen Benutzern und Virtual Delivery Agents (VDAs) mit den folgenden Schritten:
  - Konfigurieren Sie TLS auf den Maschinen, auf denen die VDAs installiert sind. (Der Einfachheit halber werden nachfolgend Maschinen, auf denen VDAs installiert sind, als "VDAs" bezeichnet.) Sie können ein PowerShell-Skript von Citrix verwenden oder eine manuelle Konfiguration vornehmen. Allgemeine Informationen finden Sie unter TLS-Einstellungen auf VDAs. Detaillierte Informationen finden Sie unter Konfigurieren von auf einem VDA mit dem PowerShell-Skript und Manuelle Konfiguration von TLS auf einem VDA.
  - Konfigurieren Sie SSL in den Bereitstellungsgruppen, die die VDAs enthalten, indem Sie eine Reihe von PowerShell-Cmdlets in Studio ausführen. Einzelheiten finden Sie unter Konfigurieren von TLS auf Bereitstellungsgruppen.

  Anforderungen und Überlegungen:
  - Das Aktivieren von TLS-Verbindungen zwischen Benutzern und VDAs gilt nur für XenApp 7.6- und XenDesktop 7.6-Sites sowie für unterstützte höhere Releases.
  - Konfigurieren Sie TLS in den Bereitstellungsgruppen und auf den VDAs nach der Installation von Komponenten sowie nach dem Erstellen von Sites, Maschinenkatalogen und Bereitstellungsgruppen.
  - Zum Konfigurieren von TLS in den Bereitstellungsgruppen müssen Sie die Berechtigung zum Ändern der Zugriffsregeln für Controller haben; ein Volladministrator hat diese Berechtigung.
  - Zum Konfigurieren von TLS auf den VDAs müssen Sie ein Windows-Administrator auf der Maschine sein, auf der der VDA installiert ist.
  - Wenn Sie TLS auf VDAs konfigurieren möchten, für die ein Upgrade von einer früheren Version durchgeführt wurde, deinstallieren Sie die SSL-Relay-Software vor dem Upgrade von den Maschinen.
  - Das PowerShell-Skript konfiguriert TLS auf statischen VDAs, jedoch nicht auf gepoolten VDAs, die von Maschinenerstellungsdienste oder Provisioning Services bereitgestellt wurden und deren Maschinenimage bei jedem Neustart zurückgesetzt wird.

Beachten Sie Folgendes beim Arbeiten in der Windows-Registrierung:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.
Weitere Informationen zur Aktivierung von TLS auf der Sitedatenbank finden Sie unter CTX137556.

## Installieren von TLS-Serverzertifikaten auf Controllern

Für HTTPS wird TLS vom XML-Dienst über Serverzertifikate, nicht aber über Clientzertifikate unterstützt. Nachfolgend finden Sie Anleitungen zum Abrufen eines Zertifikats und zur Installation und Registrierung auf einem Controller sowie zum Konfigurieren eines Ports mit dem SSL-Zertifikat:

- Wenn IIS auf dem Controller installiert ist, folgen Sie den Anleitungen unter https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- Wenn der Controller nicht über IIS verfügt, können Sie das Zertifikat mit folgender Methode konfigurieren:
  1. Rufen Sie ein SSL-Serverzertifikat ab und installieren Sie es auf dem Controller, wie unter http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx beschrieben. Weitere Informationen zum certreq-Tool finden Sie unter http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
     Wenn Sie TLS auf VDAs mit dem PowerShell-Skript konfigurieren und dabei den Fingerabdruck des SSL-Zertifikats nicht angeben, stellen Sie sicher, dass das Zertifikat im Zertifikatspeicher unter "Lokaler Computer > Eigene Zertifikate > Zertifikate" gespeichert ist. Wenn mehrere Zertifikate in dem Speicherort sind, wird das zuerst gefundene verwendet.

  2. Konfigurieren Sie einen Port mit dem Zertifikat. Weitere Informationen finden Sie unter http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

## Ändern von HTTP- oder HTTPS-Ports

Der XML-Dienst hört standardmäßig Port 80 auf HTTP-Datenverkehr und Port 443 auf HTTPS-Datenverkehr ab. Zwar können auch andere Ports verwendet werden, jedoch wird der Controller dabei nicht vertrauenswürdigen Netzwerken ausgeliefert, und es entsteht ein Sicherheitsrisiko. Das Bereitstellen eines eigenständigen StoreFront-Servers ist dem Ändern der Standardwerte vorzuziehen.
Zum Ändern der vom Controller verwendeten standardmäßigen HTTP- oder HTTPS-Ports führen Sie den folgenden Befehl in Studio aus: BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>

<http-port> ist die Portnummer für HTTP-Datenverkehr und <https-port> ist die Portnummer für HTTPS-Datenverkehr.

Hinweis: Nachdem Sie einen Port geändert haben, zeigt Studio möglicherweise eine Meldung zu Lizenzkompatibilität und Upgrades an. Sie lösen das Problem, indem Sie Dienstinstanzen mit den folgenden PowerShell-Cmdlets neu registrieren:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding  XML_HTTPS | Unregister-ConfigRegisteredServiceInstance Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |  Regist
```

## Erzwingen von HTTPS-Datenverkehr

Wenn der XML-Dienst den HTTP-Datenverkehr ignorieren soll, legen Sie den folgenden Registrierungswert unter HKLM\Software\Citrix\DesktopServer\ auf dem Controller fest und starten Sie den Brokerdienst neu.

Um den HTTP-Datenverkehr zu ignorieren, legen Sie für XmlServicesEnableNonSsl 0 fest.

Es gibt einen entsprechenden Registrierungswert, damit der HTTPS-Datenverkehr ignoriert wird: XmlServicesEnableSsl. Stellen Sie sicher, dass er nicht auf 0 festgelegt ist.

## TLS-Einstellungen auf VDAs

Wenn Sie TLS auf VDAs konfigurieren, werden Berechtigungen auf dem installierten SSL-Zertifikat geändert. Der ICA-Dienst erhält Lesezugriff für den privaten Schlüssel des Zertifikats und informiert den ICA-Dienst über Folgendes:

- **Das für TLS zu verwendende Zertifikat im Zertifikatspeicher**
- **Die für TLS-Verbindungen zu verwendende TCP-Portnummer**
  Die Windows-Firewall (wenn sie aktiviert ist) muss so konfiguriert sein, dass eingehende Verbindungen auf diesem TCP-Port zugelassen sind. Diese Konfiguration wird für Sie ausgeführt, wenn Sie das PowerShell-Skript verwenden.

- **Die zulässigen Versionen des TLS-Protokolls**

> Important


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix empfiehlt seinen Kunden den Einsatz von SSL Version 3 zu prüfen und die Konfiguration von Bereitstellungen soweit möglich dahingehend zu ändern, dass SSL Version 3 nicht mehr unterstützt wird. Weitere Informationen finden Sie unter CTX200238.

Die unterstützten SSL-Protokollversionen unterliegen einer Hierarchie (von der niedrigsten zur höchsten Version): TLS 3.0, TLS 1.0, TLS 1.1 und TLS 1.2. Wenn Sie die zulässige Mindestversion angeben, sind alle Protokollverbindungen, die diese Version oder eine höhere Version verwenden, zulässig.

Wenn Sie beispielsweise TLS 1.1 als Mindestversion angeben, werden auch TLS 1.1- und TLS 1.2-Protokollverbindungen zugelassen. Wenn Sie SSL 3.0 als Mindestversion angeben, sind Verbindungen für alle unterstützten Versionen zulässig. Wenn Sie TLS 1.2 als Mindestversion angeben, werden nur TLS 1.2-Verbindungen zugelassen.

- **Die zulässigen TLS-Verschlüsselungsverfahren**
  Eine Verschlüsselungssammlung ist eine Liste gebräuchlicher TLS-Verschlüsselungsverfahren. Wenn ein Client eine Verbindung herstellt und eine Liste unterstützter TLS-Verschlüsselungsverfahren übermittelt, ordnet der VDA ein Verschlüsselungsverfahren des Clients einem Verschlüsselungsverfahren in der konfigurierten Verschlüsselungssammlung zu und akzeptiert die Verbindung. Wenn der Client ein Verschlüsselungsverfahren übermittelt, das nicht in der Verschlüsselungssammlung des VDAs ist, lehnt der VDA die Verbindung ab.

  Drei Verschlüsselungssammlungen werden unterstützt: GOV (Government), COM (Commercial) und ALL. Die Verschlüsselungsverfahren in diesen Verschlüsselungssammlungen hängen vom Windows FIPS-Modus ab. Weitere Informationen zum Windows FIPS-Modus finden Sie unter http://support.microsoft.com/kb/811833. In der folgenden Tabelle finden Sie die für die jeweilige Verschlüsselungssammlung unterstützten Verschlüsselungsverfahren.

| **TLS-Verschlüsselungssammlung** | GOV | COM | ALL | GOV | COM | ALL |
|---|---|---|---|---|---|---|
| **FIPS-Modus** | Off | Off | Off | On | On | On |
| **RSA_KEYX** | x | x | x | x | x | x |
| **RSA_SIGN** | x | x | x | x | x | x |
| **3DES** | x | | x | x | | x |
| **RC4** | | x | x | | | |
| **MD5** | x | x | x | | | |
| **SHA** | x | x | x | x | x | x |
| **SHA_256** | x | x | x | x | x | x |
| **SHA_384** | x | x | x | x | x | x |
| **SHA_512** | x | x | x | x | x | x |
| **AES** | x | x | x | x | x | x |

Eine Bereitstellungsgruppe darf nicht eine Mischung von VDAs mit und ohne konfiguriertem TLS enthalten. Wenn Sie TLS für eine Bereitstellungsgruppe konfigurieren, sollten Sie TLS bereits für alle VDAs in dieser Bereitstellungsgruppe konfiguriert haben.

### Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript

Das Skript Enable-VdaSSL.ps1 aktiviert oder deaktiviert den TLS-Listener auf einem VDA. Dieses Skript ist im Ordner Support > Tools > SslSupport auf dem Installationsmedium verfügbar.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für den angegebenen TCP-Port. Dann wird eine Regel hinzugefügt, die dem ICA-Dienst die Annahme eingehender Verbindungen nur auf dem TLS-TCP-Port gewährt. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Citrix ICA (Standard: 1494)
- Citrix CGP (Standard: 2598)
- Citrix WebSocket (Standard: 8008)

Als Folge können Benutzer Verbindungen nur über TLS herstellen und nicht über unformatiertes ICA, CGP oder WebSocket.

Das Skript enthält die folgenden Syntax-Beschreibungen sowie zusätzliche Beispiele. Sie können diese Informationen mit einem Tool wie Notepad++ überprüfen.

Sie müssen einen der Parameter –Enable oder –Disable angeben, alle anderen Parameter sind optional.

**Syntax**

Enable-VdaSSL {-Enable | -Disable} [–SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"<suite>"] [-CertificateThumbPrint "<thumbprint>"]

| **Parameter** | **Beschreibung** |
|---|---|
| -Enable | Installiert und aktiviert den TLS-Listener auf dem VDA. Dieser Parameter oder der Parameter –Disable ist erforderlich. |
| -Disable | Deaktiviert den TLS-Listener auf dem VDA. Dieser Parameter oder der Parameter –Enable ist erforderlich. Wenn Sie diesen Parameter festlegen, sind keine anderen Parameter gültig. |
| –SSLPort <port> | TLS port: Standard: 443 |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Parameter | Beschreibung |
|---|---|
| -SSLMinVersion "<min-ssl-version>" | Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: "SSL_3.0", "TLS_1.0", "TLS_1.1" und "TLS_1.2". Standard: "TLS_1.0"<br><br>**Wichtig:** Citrix empfiehlt seinen Kunden den Einsatz von SSL Version 3 zu prüfen und die Konfiguration von Bereitstellungen möglichst dahingehend zu ändern, dass SSL Version 3 nicht mehr unterstützt wird. Weitere Informationen finden Sie unter CTX200238. |
| -SSLCipherSuite "<suite>" | TLS-Verschlüsselungssammlung zwischen Anführungszeichen. Gültige Werte: "GOV", "COM" und "ALL". Standard: "ALL" |
| -CertificateThumbPrint "<thumbprint>" | Fingerabdruck des SSL-Zertifikats im Zertifikatspeicher, zwischen Anführungszeichen. Dieser Parameter wird normalerweise verwendet, wenn der Zertifikatspeicher über mehrere Zertifikate verfügt. Das Skript verwendet den Fingerabdruck, um das gewünschte Zertifikat auszuwählen. Standard: das erste verfügbare Zertifikat im Bereich "Lokaler Computer > Eigene Zertifikate > Zertifikate" des Zertifikatspeicher. |

**Beispiele**

Das folgende Skript installiert und aktiviert den TLS 1.2-Versionswert.

```
Enable-VdaSSL –Enable
```

Das folgende Skript installiert und aktiviert den TLS-Listener und gibt den TLS-Port 400 an sowie die Verschlüsselungssammlung GOV und als Mindestprotokollversion "TLS 1.2 TLS".

```
Enable-VdaSSL – Enable –SSLPort 400 'SSLMinVersion "TLS_1.2"  –SSLCipherSuite "GOV"
```

Das folgende Skript deaktiviert den TLS-Listener auf dem VDA.

```
Enable-VdaSSL –Disable
```

### Manuelle Konfiguration von TLS auf einem VDA

Bei der manuellen Konfiguration von TLS auf einem VDA gewähren Sie dem privaten Schlüssel des TLS-Zertifikats allgemeinen Lesezugriff für den entsprechenden Dienst auf jedem VDA: NT SERVICE\PorticaService für einen VDA für Windows-Desktopbetriebssysteme oder NT SERVICE\TermService für einen VDA für Windows-Serverbetriebssysteme. Führen Sie auf der Maschine, auf der der VDA installiert ist, folgende Schritte aus:

1. Starten Sie die Microsoft Management Console (MMC): Start > Ausführen > mmc.exe.
2. Fügen Sie dem MMC das Zertifikat-Snap-In hinzu:
   1. Wählen Sie Datei > Snap-In hinzufügen/entfernen.
   2. Wählen Sie Zertifikate aus und klicken Sie auf Hinzufügen.
   3. Wählen Sie unter "Dieses Snap-In verwaltet die Zertifikate für:" die Option Computerkonto und klicken Sie dann auf Weiter.
   4. Wählen Sie unter "Wählen Sie den Computer aus, den dieses Snap-In verwalten soll" die Option Lokalen Computer und klicken Sie dann auf Fertig stellen.
3. Klicken Sie unter "Zertifikate (Lokaler Computer) > Eigene Zertifikate > Zertifikate" mit der rechten Maustaste auf das Zertifikat und wählen Sie Alle Aufgaben > Private Schlüssel verwalten.
4. Im Zugriffssteuerungslisten-Editor wird "Permissions for <Anzeigename> private keys" angezeigt, wobei <Anzeigename> der Name des SSL-Zertifikats ist. Fügen Sie einen der folgenden Dienste hinzu und geben Sie ihm Lesezugriff:
   - Für einen VDA für Windows-Desktopbetriebssysteme "PORTICASERVICE"
   - Für einen VDA für Windows-Serverbetriebssysteme "TERMSERVICE"
5. Doppelklicken Sie auf das installierte SSL-Zertifikat. Wählen Sie im Dialogfeld des Zertifikats die Registerkarte "Details" aus und führen Sie einen Bildlauf nach unten durch. Klicken Sie auf Fingerabdruck.
6. Führen Sie regedit aus und navigieren Sie zu HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
   1. Bearbeiten Sie den SSL-Fingerabdruckschlüssel und kopieren Sie den Fingerabdruckwert des SSL-Zertifikats in den binären Wert. Sie können unbekannte Elemente im Dialogfeld Binärwert bearbeiten ignorieren (z. B. "0000" und Sonderzeichen).
   2. Bearbeiten Sie den Schlüssel "SSLEnabled" und ändern Sie den Wert für DWORD in "1". (Um SSL zu einem späteren Zeitpunkt zu deaktivieren, ändern Sie den Wert für DWORD in "0&".)
   3. Wenn Sie die Standardeinstellungen ändern möchten (optional), verwenden Sie Folgendes im gleichen Registrierungspfad:
      - SSLPort DWORD – SSL-Portnummer. Standard: 443.
      - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Standard: 2 (TLS 1.0).
      - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Standard: 3 (ALL).
7. Stellen Sie sicher, dass der TLS-TCP-Port in der Windows-Firewall geöffnet ist, wenn Sie nicht den Standardport 443 verwenden. (Wenn Sie die eingehende Regel für die Windows-Firewall erstellen, wählen Sie in den Eigenschaften die Optionen "Verbindung zulassen" und "Aktiviert" aus.)
8. Stellen Sie sicher, dass keine anderen Anwendungen oder Dienste (z. B. IIS) den TLS-TCP-Port verwenden.
9. Damit die Änderungen auf VDAs für Windows-Serverbetriebssysteme wirksam werden, starten Sie die Maschine neu. (Sie brauchen Maschinen mit VDAs für Windows-Desktopbetriebssysteme nicht neu starten.)

### Konfigurieren von TLS auf Bereitstellungsgruppen

Führen Sie diese Schritte für jede Bereitstellungsgruppe aus, die VDAs enthält, die Sie für TLS-Verbindungen konfiguriert haben.

1. Öffnen Sie in Studio die PowerShell-Konsole.
2. Führen Sie asnp Citrix.* aus, um die Citrix Produkt-Cmdlets zu laden.
3. Führen Sie Get-BrokerAccessPolicyRule -DesktopGroupName '<delivery-group-name>' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true aus.
   <delivery-group-name> ist der Name der Bereitstellungsgruppe mit den VDAs.
4. Führen Sie Set-BrokerSite –DnsResolutionEnabled $true aus.

### Problembehandlung

Wenn ein Verbindungsfehler auftritt, überprüfen Sie Systemereignisprotokoll des VDAs.

Wenn Sie Citrix Receiver für Windows verwenden und ein Verbindungsfehler auftritt (z. B. 1030), der auf einen TLS-Fehler hinweist, deaktivieren Sie Desktop Viewer und versuchen Sie erneut, die Verbindung herzustellen. Der Verbindungsfehler tritt zwar immer noch auf, aber u. U. wird eine Erklärung zu dem zugrunde liegenden TLS-Fehler angegeben (z. B. dass Sie beim Anfordern eines Zertifikats von der Zertifizierungsstelle die falsche Vorlage angegeben haben).

## Kommunikation zwischen Controller und VDA

Die Kommunikation zwischen Controller und VDA wird auf Nachrichtenebene durch Windows Communication Framework (WCF) gesichert. Zusätzlicher Schutz auf Übertragungsebene durch TLS ist nicht erforderlich. Die WCF-Konfiguration verwendet Kerberos für die gegenseitige Authentifizierung von Controller und VDA. Die Verschlüsselung verwendet AES im CBC-Modus mit einem 256-Bit-Schlüssel. Für die Nachrichtenintegrität wird SHA-1 verwendet.

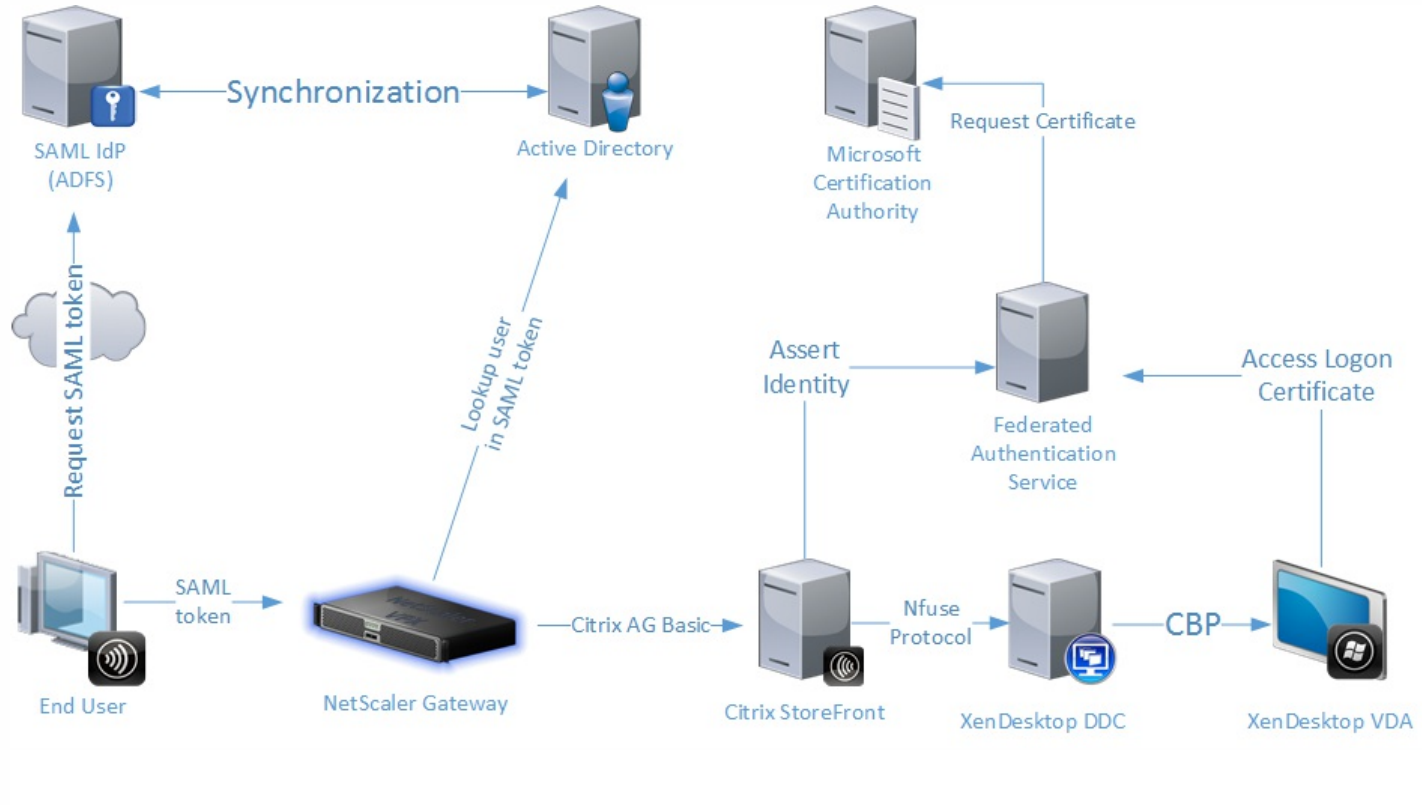

© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Federated Authentication Service

Jul 13, 2016

Citrix Federated Authentication Service ist eine privilegierte Komponente für die Integration in Active Directory-Zertifikatdienste. Der Dienst stellt dynamisch Zertifikate für Benutzer aus, sodass diese sich bei einer Active Directory-Umgebung so anmelden können, als hätten sie eine Smartcard. Dadurch kann in StoreFront eine größere Bandbreite an Authentifizierungsoptionen, darunter z. B. SAML-Assertionen, verwendet werden. SAML (Security Assertion Markup Language) wird häufig als Alternative für herkömmliche Windows-Benutzerkonten im Internet verwendet.

Die folgende Abbildung zeigt das Zusammenwirken von Federated Authentication Service mit einer Microsoft-Zertifizierungsstelle und die Bereitstellung entsprechender Dienste für StoreFront sowie XenApp- und XenDesktop-VDAs.




Vertrauenswürdige StoreFront-Server kontaktieren den Federated Authentication Service (FAS), wenn Benutzer Zugriff auf die Citrix Umgebung anfordern. Der FAS stellt ein Ticket aus, mit dem eine einzelne XenApp- oder XenDesktop-Sitzung eine Authentifizierung mit einem Zertifikat für die Sitzung durchführen kann. Wenn ein VDA einen Benutzer authentifizieren muss, stellt er eine Verbindung mit dem FAS her und löst das Ticket aus. Nur der FAS hat Zugriff auf den privaten Schlüssel des Benutzerzertifikats. Der VDA muss jeden erforderlichen Signier- und Entschlüsselungsvorgang mit dem Zertifikat an den FAS senden.

# Anforderungen

Der Federated Authentication Service wird unter Windows Server-Betriebssystemen (Windows Server 2008 R2 oder höher) unterstützt.

- Citrix empfiehlt die Installation des FAS auf einem Server, der keine anderen Citrix Komponenten enthält.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Der Windows-Server muss geschützt werden. Er erhält Zugriff auf ein Registrierungsstellenzertifikat und einen privaten Schlüssel zur automatischen Ausstellung von Zertifikaten für die Domänenbenutzer und Zugriff auf diese Benutzerzertifikate und privaten Schlüssel.

XenApp- bzw. XenDesktop-Site

- Die Delivery Controller müssen mindestens in Version 7.9 vorliegen.
- Die VDAs müssen mindestens in Version 7.9 vorliegen. Vergewissern Sie sich, dass die Federated Authentication Service-Gruppenrichtlinienkonfiguration richtig auf die VDAs angewendet wurde, bevor Sie den Maschinenkatalog gemäß dem Standardverfahren erstellen. Einzelheiten finden Sie in dem Abschnitt zum Konfigurieren der Gruppenrichtlinien.
- Der StoreFront-Server muss mindestens in Version 3.6 vorliegen (dies ist die im ISO-Image für XenApp-/XenDesktop 7.9 enthaltene Version).

Konsultieren Sie bei der Planung der Bereitstellung dieses Diensts den Abschnitt "Sicherheitsüberlegungen".

Informationsquellen:

- Active Directory-Zertifikatdienste

  https://technet.microsoft.com/en-us/library/hh831740.aspx

- Konfigurieren von Windows für die Zertifikatanmeldung

  http://support.citrix.com/article/CTX206156

# Reihenfolge der Schritte zur Installation und Einrichtung

1. Installieren des Federated Authentication Service
2. Aktivieren des Plug-Ins für den Federated Authentication Service auf StoreFront-Servern
3. Konfigurieren der Gruppenrichtlinie
4. Verwenden Sie die Federated Authentication Service-Verwaltungskonsole für folgende Aufgaben: (a) Bereitstellen der vorhandenen Vorlagen, (b) Einrichten von Zertifizierungsstellen und (c) Autorisieren des Federated Authentication Service für die Verwendung der Zertifizierungsstelle.
5. Konfigurieren von Benutzerregeln

# Sicherheitsüberlegungen Federated Authentication Service

Aus Sicherheitsgründen empfiehlt Citrix die Installation des FAS auf einem dedizierten Server, der ähnlich geschützt wird wie ein Domänencontroller oder eine Zertifizierungsstelle. Der FAS kann über die Schaltfläche **Federated Authentication Service** auf dem Begrüßungsbildschirm der automatischen Ausführung beim Einfügen der ISO-Datei installiert werden.

Es werden folgende Komponenten installiert:

- Federated Authentication Service


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- PowerShell-Snap-In-Cmdlets zur Remote-Konfiguration des Federated Authentication Service
- Verwaltungskonsole des Federated Authentication Service
- Gruppenrichtlinienvorlagen für den Federated Authentication Service (CitrixFederatedAuthenticationService.admx/adml)
- Zertifikatvorlagendateien zur einfachen Konfiguration einer Zertifizierungsstelle
- Leistungsindikatoren und Ereignisprotokolle

# Aktivieren des Plug-Ins für den Federated Authentication Service für einen StoreFront-Store

Zum Aktivieren der FAS-Integration auf einem StoreFront-Store führen Sie die folgenden PowerShell-Cmdlets als Administrator aus. Wenn Sie mehrere Stores haben oder der Store einen anderen Namen hat, kann der Pfad von dem unten angegebenen abweichen.

command KOPIEREN

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "FASLogonDataProvider"
```

Zum Beenden der Verwendung des FAS verwenden Sie folgendes PowerShell-Skript:

command KOPIEREN


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

# Konfigurieren des Delivery Controllers

Zur Verwendung des Federated Authentication Service konfigurieren Sie den XenApp- bzw. XenDesktop-Delivery Controller für eine Vertrauensstellung mit den StoreFront-Servern, die mit ihm eine Verbindung herstellen können. Führen Sie hierfür das PowerShell-Cmdlet **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** aus.

# Konfigurieren der Gruppenrichtlinie

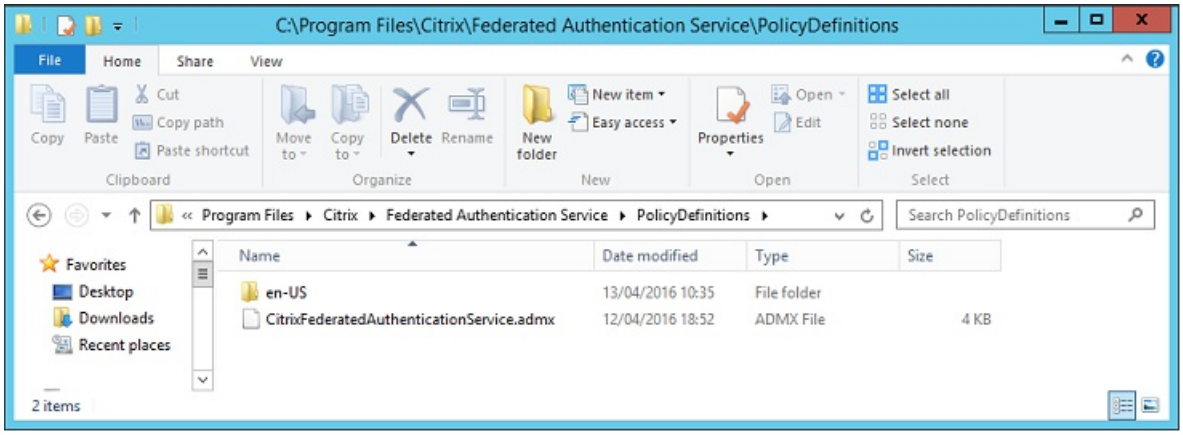
Nach der Installation des Federated Authentication Service müssen Sie die vollständigen DNS-Adressen der FAS-Server in der Gruppenrichtlinie unter Verwendung der im Installationsprogramm enthaltenen Gruppenrichtlinienvorlagen angeben.

**Wichtig:** Die Tickets anfordernden StoreFront-Server und die Tickets auslösenden VDAs müssen die gleiche DNS-Adresskonfiguration haben, einschließlich der automatischen Servernummerierung, die vom Gruppenrichtlinienobjekt angewendet wird.

Der Einfachheit halber zeigen die folgenden Beispiele die Konfiguration einer Richtlinie auf Domänenebene für alle Maschinen. Dies ist jedoch nicht erforderlich. Der FAS funktioniert, wenn die Liste der DNS-Adressen für die StoreFront-Server, die VDAs und die Maschine mit der FAS-Verwaltungskonsole identisch sind. Von dem Gruppenrichtlinienobjekt wird jedem Eintrag eine Indexnummer hinzugefügt. Diese Nummern müssen, wenn mehrere Objekte verwendet werden, ebenfalls übereinstimmen.

**Schritt 1:** Suchen Sie auf dem Server, auf dem Sie den FAS installiert haben, die Datei C:\Programme\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx und dann den Ordner "de-DE".

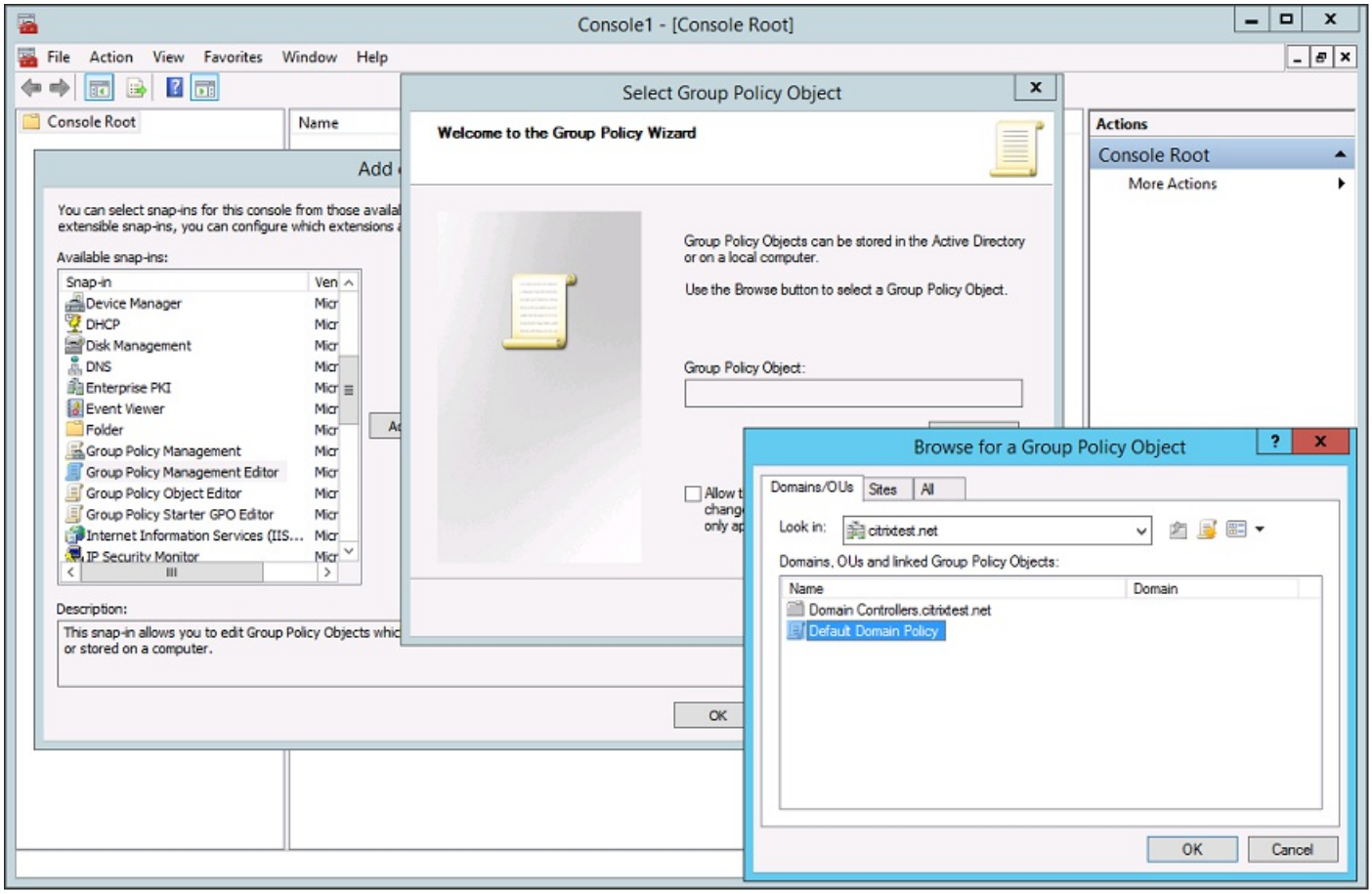

© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Schritt 2:** Kopieren Sie beide auf den Domänencontroller in den Pfad C:\Windows\PolicyDefinitions.

**Schritt 3:** Führen Sie Microsoft Management Console (Befehlszeile: "mmc.exe") aus. Klicken Sie auf der Menüleiste auf **Datei > Snap-In hinzufügen/entfernen**. Fügen Sie den Gruppenrichtlinienverwaltungs-Editor hinzu.

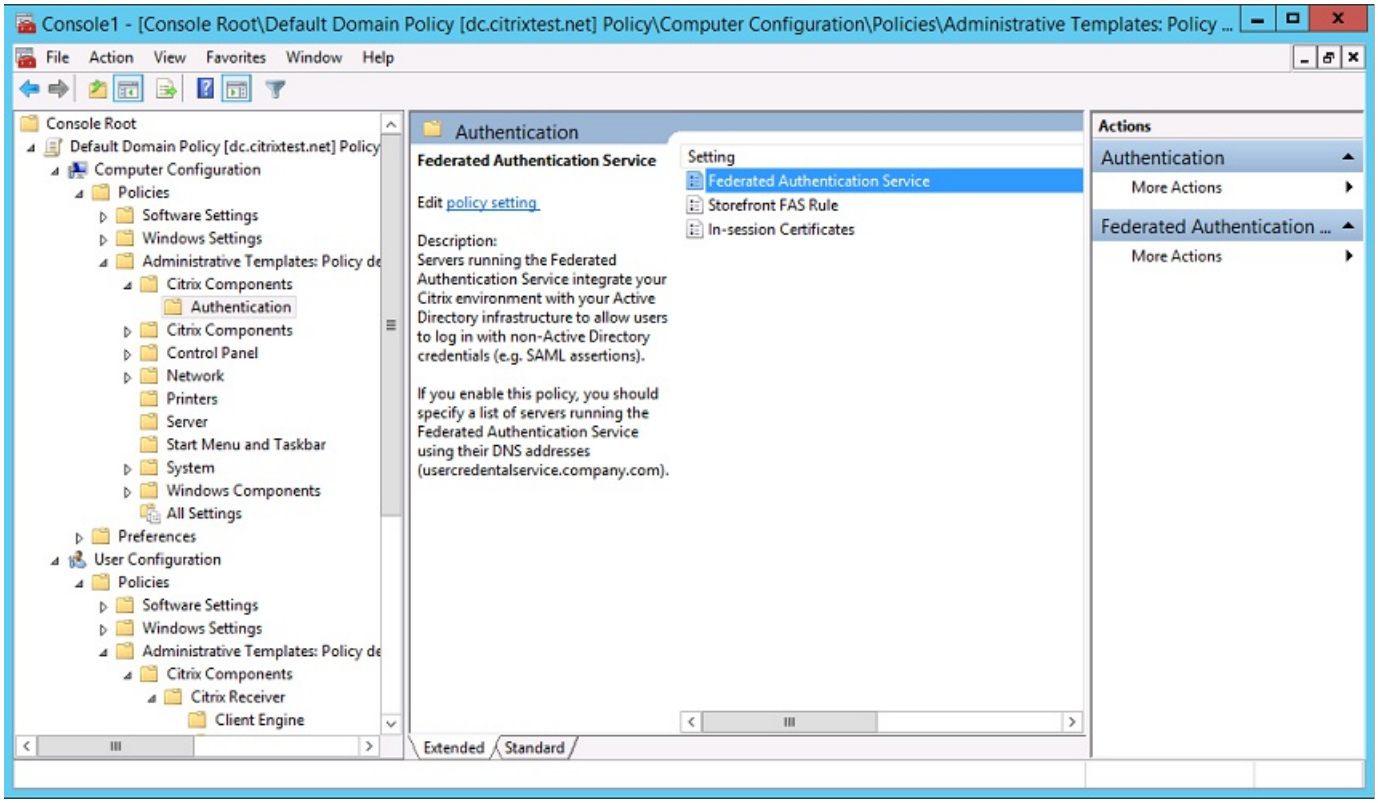
Wenn Sie zur Angabe eines Gruppenrichtlinienobjekts aufgefordert werden, klicken Sie auf **Durchsuchen** und wählen Sie **Standarddomänenrichtlinie**. Alternativ können Sie ein für Ihre Umgebung geeignetes Richtlinienobjekt mit einem Tool Ihrer Wahl erstellen und auswählen. Die Richtlinie muss auf alle Maschinen angewendet werden, auf denen relevante Citrix Software (VDAs, StoreFront-Server, Verwaltungstools) ausgeführt wird.





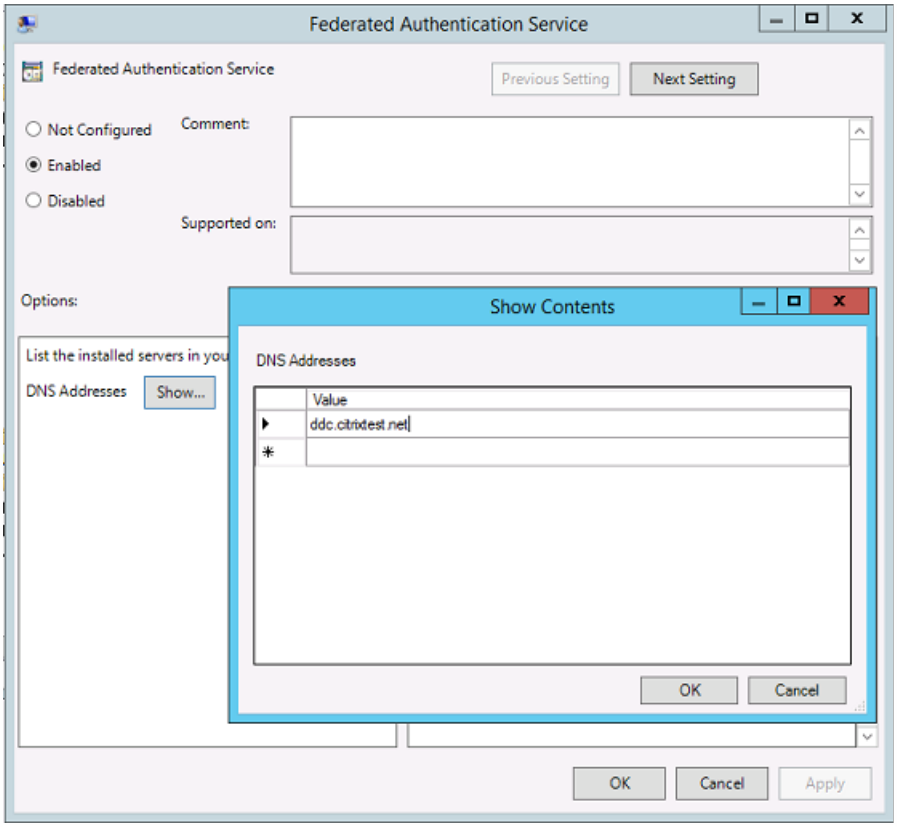
© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Schritt 4:** Navigieren Sie zu der Federated Authentication Service-Richtlinie unter Configuration/Policies/Administrative Templates/Citrix Components/Authentication.




**Schritt 5:** Öffnen Sie die Federated Authentication Service-Richtlinie und wählen Sie **Aktiviert**. Damit können Sie auf die Schaltfläche **Anzeigen** klicken und die DNS-Adressen der FAS-Server konfigurieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Schritt 6:** Geben Sie die DNS-Adressen der Server ein, auf denen der Federated Authentication Service gehostet wird.

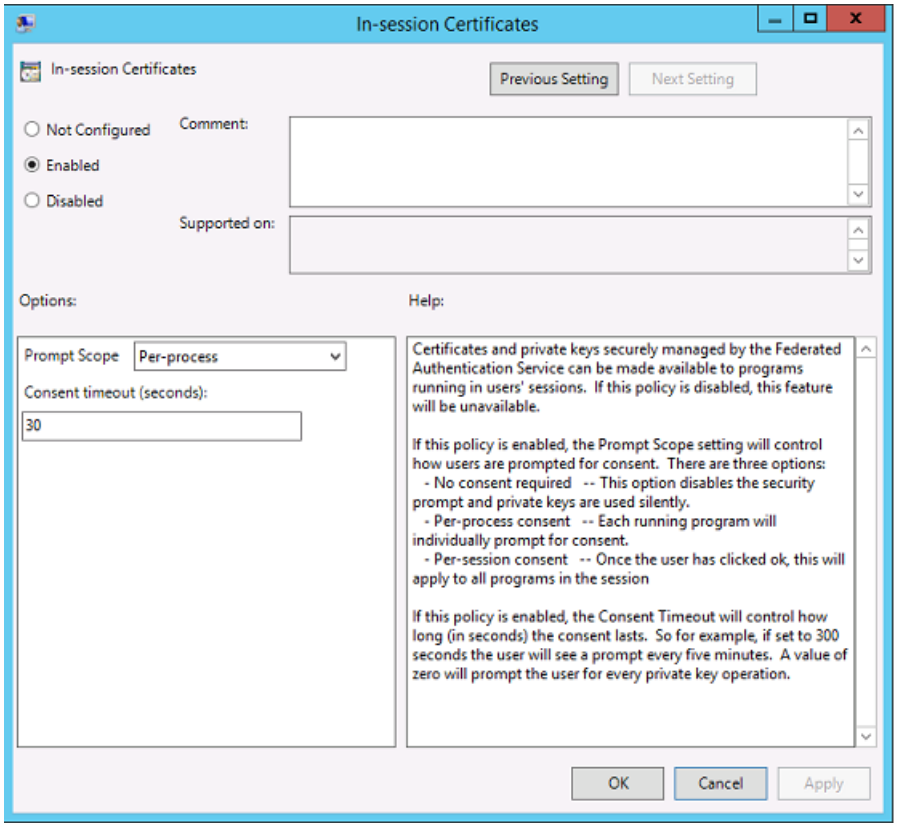
**Hinweis:** Wenn Sie mehrere Adressen eingeben, muss deren Reihenfolge auf der Liste für StoreFront-Server und VDAs identisch sein. Dies gilt auch für leere bzw. nicht verwendete Listeneinträge.

**Schritt 7:** Klicken Sie auf **OK**, um den Assistenten für die Gruppenrichtlinie zu schließen und die Änderungen anzuwenden. Sie müssen u. U. die Maschinen neu starten oder **gpupdate /force** an der Befehlszeile ausführen, damit die Änderungen wirksam werden.

## Aktivieren der Unterstützung für sitzungsinterne Zertifikate

Die Gruppenrichtlinienvorlage umfasst Unterstützung zur Konfiguration des Systems für sitzungsinterne Zertifikate. Damit werden Zertifikate nach der Anmeldung eines Benutzers in dessen persönlichem Zertifikatspeicher abgelegt. Ein Zertifikat kann dann beispielsweise von Internet Explorer verwendet werden, wenn innerhalb der VDA-Sitzung eine TLS-Authentifizierung bei Webservern erforderlich ist. Standardmäßig gestatten VDAs keinen Zugriff auf Zertifikate nach der Anmeldung.

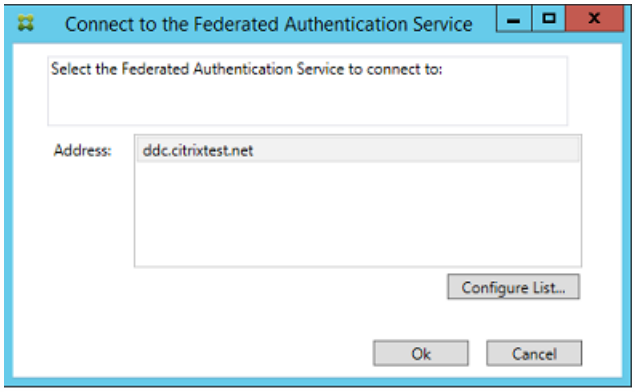

© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Verwendung der FAS-Verwaltungskonsole

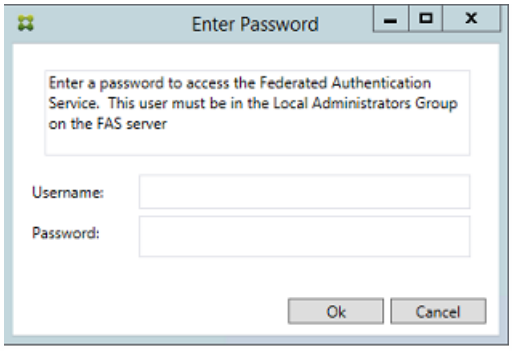
Die FAS-Verwaltungskonsole wird zusammen mit dem Federated Authentication Service installiert. Ein Symbol (Citrix Federated Authentication Service) wird in das Startmenü eingefügt.

Es wird automatisch versucht, die FAS-Server in der Umgebung mithilfe der Gruppenrichtlinie zu lokalisieren. Wenn dies fehlschlägt, konsultieren Sie den Abschnitt Konfigurieren der Gruppenrichtlinie.

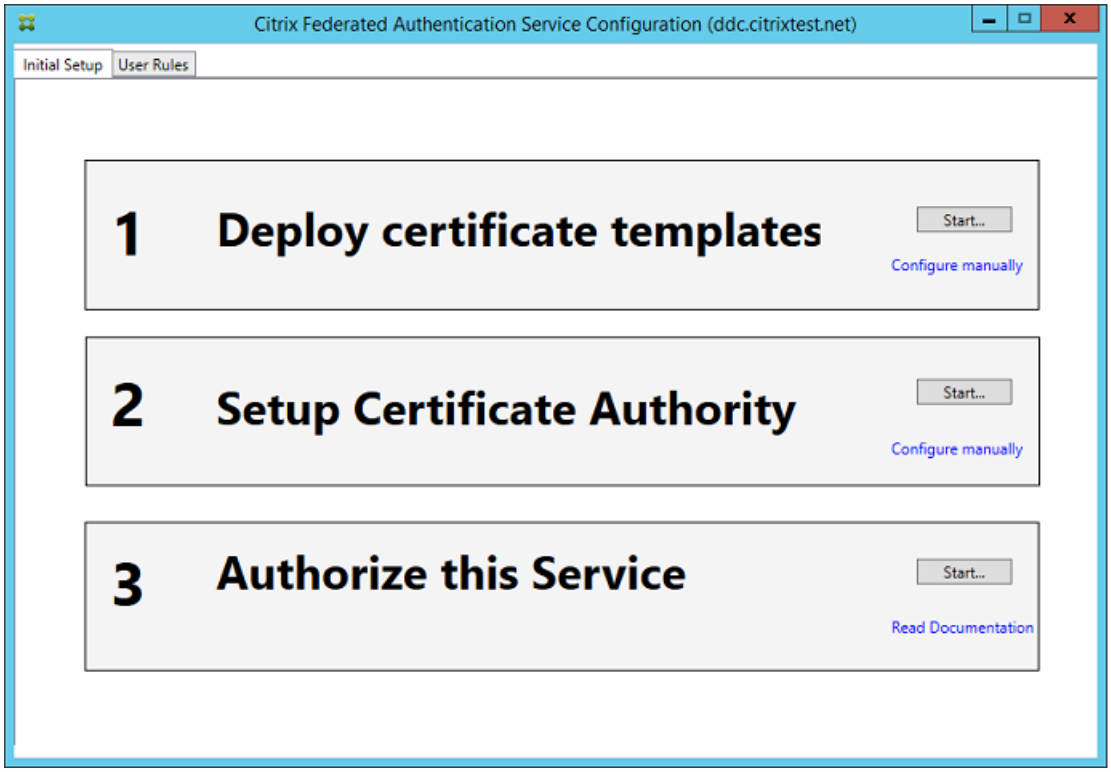



Wenn Ihr Benutzerkonto nicht Mitglied der Administratorengruppe auf dem Computer mit dem Federated Authentication Service ist, werden Sie zur Eingabe von Anmeldeinformationen aufgefordert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Bei der ersten Verwendung der Verwaltungskonsole werden Sie durch ein dreiteiliges Verfahren zum Bereitstellen von Zertifikatvorlagen, Einrichten der Zertifizierungsstelle und Autorisieren des FAS für die Verwendung der Zertifizierungsstelle geführt. Einige Schritte können auch manuell mit Tools zur Betriebssystemkonfiguration durchgeführt werden.




# Bereitstellen von Zertifikatvorlagen

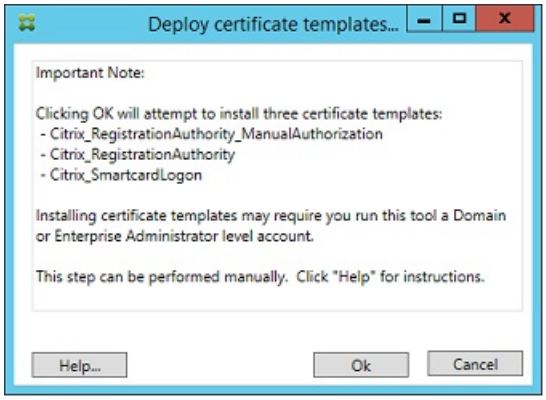
Zur Vermeidung von Interoperabilitätsproblemen mit anderer Software bietet Citrix Federated Authentication Service drei eigene Zertifikatvorlagen.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Diese Vorlagen müssen bei Active Directory registriert sein. Wenn sie von der Konsole nicht gefunden werden, können Sie sie mit dem Tool **Deploy certificate templates** installieren. Dieses Tool muss mit einem Konto ausgeführt werden, das


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administratorberechtigung für die Gesamtstruktur des Unternehmens hat.




Die Konfiguration der Vorlagen ist in den XML-Dateien mit der Erweiterung "certificatetemplate". Diese werden mit dem Federated Authentication Service in folgenden Pfad installiert:

C:\Programme\Citrix\Federated Authentication Service\CertificateTemplates

Wenn Sie keine Berechtigung zum Installieren dieser Vorlagendateien haben, geben Sie sie dem Active Directory-Administrator.

Zur manuellen Installation der Vorlagen können Sie die folgenden PowerShell-Befehle verwenden:

command KOPIEREN

```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

$CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)

$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)

$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

$writabletemplate.Commit(1, $NULL)
```

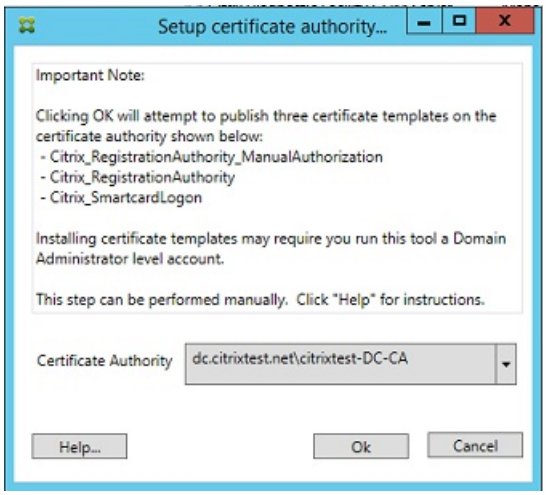
# Einrichten von Active Directory-Zertifikatdienste

Nach Installation der Citrix Zertifikatvorlagen müssen sie auf mindestens einem Microsoft-Zertifizierungsstellenserver veröffentlicht werden. Informationen zur Bereitstellung von Active Directory-Zertifikatdienste finden Sie in der Dokumentation von Microsoft.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

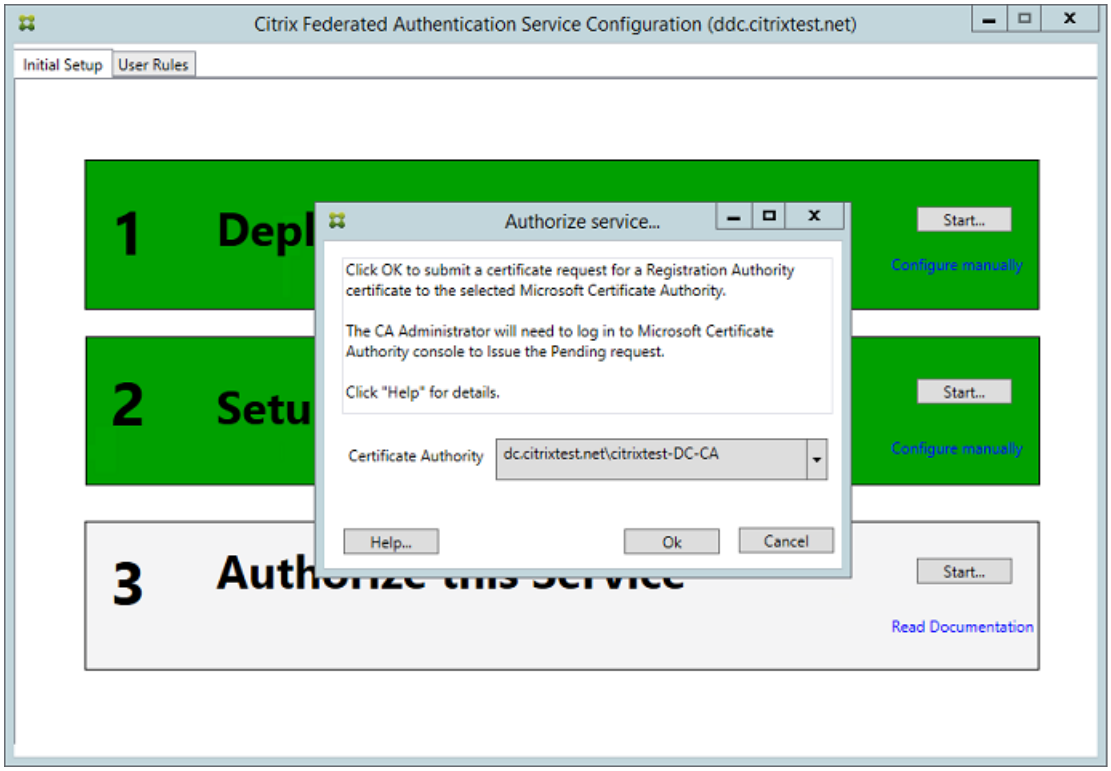
Wenn die Vorlagen nicht auf mindestens einem Server veröffentlicht werden, wird die Veröffentlichung von dem Tool **Setup certificate authority** angeboten. Sie müssen das Tool als Benutzer mit Berechtigung zum Verwalten der Zertifizierungsstelle ausführen.

(Zertifikatvorlagen können auch mit der Microsoft-Zertifizierungsstellenkonsole veröffentlicht werden.)




# Autorisieren des Federated Authentication Service

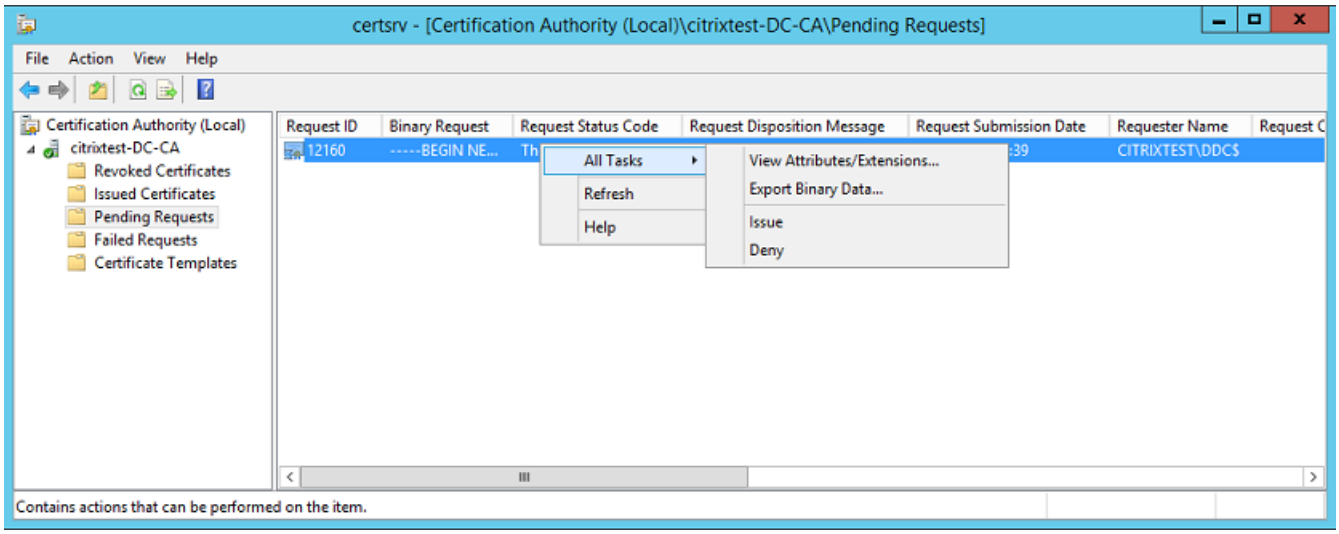
Der letzte Schritt bei der Einrichtung über die Konsole ist die Autorisierung des Federated Authentication Service. Von der Verwaltungskonsole wird die Vorlage "Citrix_RegistrationAuthority_ManualAuthorization" zum Erstellen einer Zertifikatanforderung verwendet, die dann an eine der Zertifizierungsstellen gesendet wird, die das Zertifikat veröffentlichen.



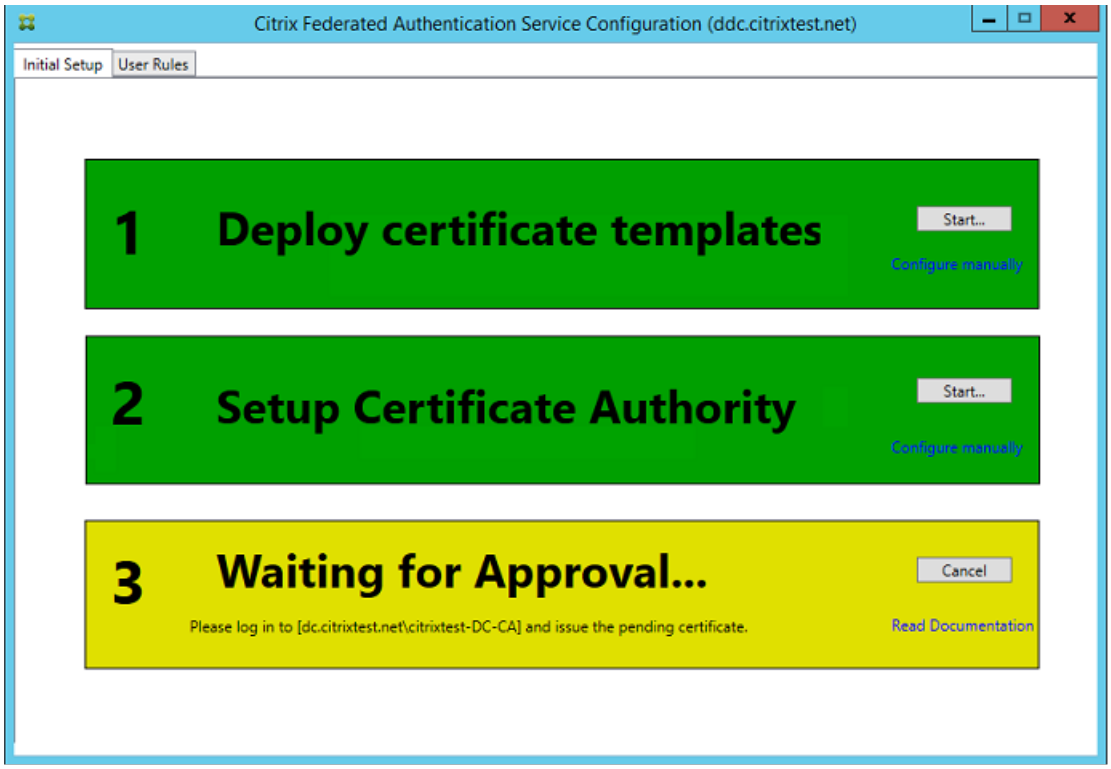


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nachdem die Anforderung gesendet wurde, wird sie in der Liste **Ausstehende Anforderungen** der Microsoft-Zertifizierungsstellenkonsole angezeigt. Der Administrator der Zertifizierungsstelle muss die Option zum Ablehnen der Anforderung oder zum Ausstellen des Zertifikats auswählen, bevor die Konfiguration des Federated Authentication Service fortgesetzt werden kann. Die Autorisierungsanforderung wird als ausstehende Anforderung vom FAS-Maschinenkonto angezeigt.




Klicken Sie mit der rechten Maustaste auf **Alle Aufgaben** und wählen Sie dann die Option **Ausstellen**oder **Verweigern** für die Zertifikatsanforderung. Die Federated Authentication Service-Verwaltungskonsole erkennt automatisch, wenn dieser Prozess abgeschlossen ist. Er kann einige Minuten dauern.



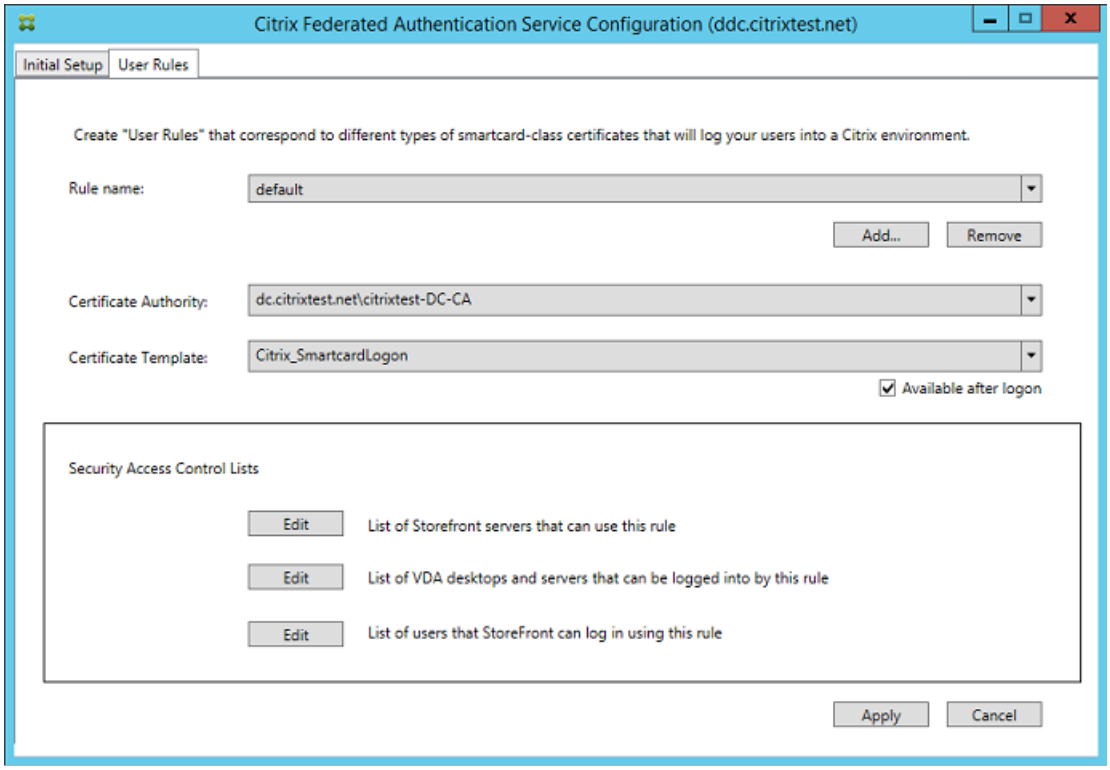


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren von Benutzerregeln

Mit Benutzerregeln wird die Ausstellung von Zertifikaten für VDA-Anmeldungen und -Sitzungen nach Vorgabe von StoreFront autorisiert. Jede Regel legt die StoreFront-Server fest, die als vertrauenswürdig zum Anfordern von Zertifikaten gelten, die Benutzer, für die sie angefordert werden können, und die VDA-Maschinen, die sie verwenden dürfen.

Zum Abschließen der Einrichtung des Federated Authentication Service muss der Administrator die Standardregel definieren, indem er in der FAS-Verwaltungskonsole zur Registerkarte "User Rules" wechselt, die Zertifizierungsstelle auswählt, in der die Vorlage "Citrix_SmartcardLogon" veröffentlicht wird, und die Liste der StoreFront-Server bearbeitet. Die Liste der VDAs enthält standardmäßig die Domänencomputer und die Liste der Benutzer die Domänenbenutzer. Die Listen können geändert werden, wenn sie nicht geeignet sind.




Felder:

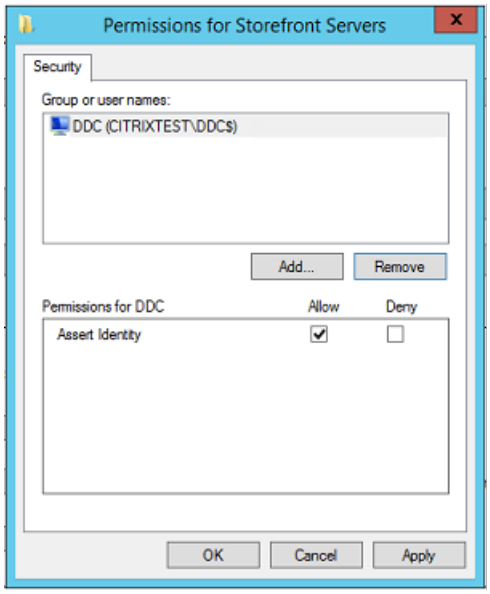
**Certificate Authority and Certificate Template**: Zertifizierungsstelle und Zertifikatvorlage, die zur Ausstellung von Benutzerzertifikaten verwendet werden sollen. Dabei muss es sich um die Vorlage "Citrix_SmartcardLogon" oder eine geänderte Kopie dieser Vorlage für eine der Zertifizierungsstellen handeln, in der die Vorlage veröffentlicht ist.

Für Failover und Lastausgleich können mehrere Zertifizierungsstellen mit PowerShell-Befehlen hinzugefügt werden. Erweiterte Optionen für die Zertifikaterstellung können über die Befehlszeile und die Konfigurationsdateien festgelegt werden. Weitere Informationen finden Sie in den Abschnitten PowerShell und Hardwaresicherheitsmodule.

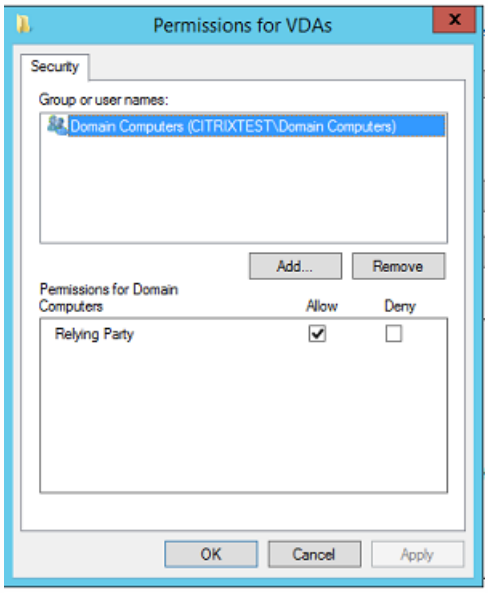
**In-Session Certificates**: Über das Kontrollkästchen **Available after logon**wird festgelegt, ob ein Zertifikat auch als sitzungsinternes Zertifikat verwendet werden kann. Wenn das Kontrollkästchen nicht aktiviert ist, wird das Zertifikat nur für Anmeldungen oder Wiederverbindungen verwendet und der Benutzer hat nach der Authentifizierung keinen Zugriff auf das Zertifikat.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**List of StoreFront servers that can use this rule**: Liste der vertrauenswürdigen StoreFront-Servermaschinen, die Zertifikate für die Anmeldung oder Wiederverbindung von Benutzern anfordern dürfen. Diese Einstellung ist sicherheitsrelevant und muss mit großer Sorgfalt gewählt werden.

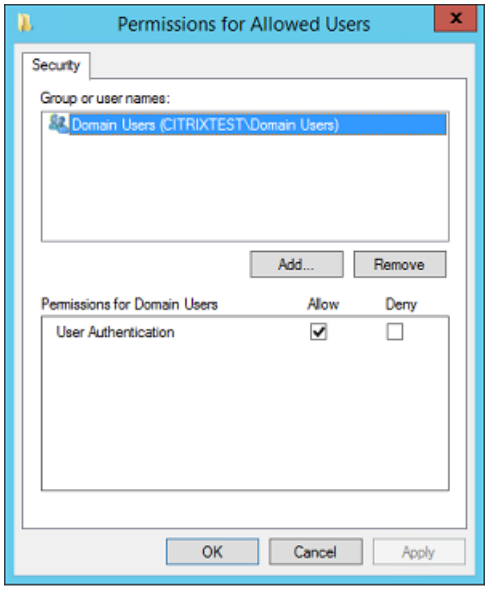



**List of VDA desktops and servers that can be logged into by this rule:** Liste der VDA-Maschinen, die Benutzer über das FAS-System anmelden dürfen.




**List of users that StoreFront can log in using this rule:** Liste der Benutzer, denen Zertifikate über den FAS ausgestellt werden dürfen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




### Erweiterte Verwendung

Sie können weitere Regeln mit Verweisen auf andere Zertifikatvorlagen und Zertifizierungsstellen mit anderen Eigenschaften und Berechtigungen einrichten. Diese Regeln können zur Verwendung durch andere StoreFront-Server konfiguriert werden, die ihrerseits zur Anforderung der neuen Regel nach deren Namen konfiguriert werden müssen. Standardmäßig fordert StoreFront beim Kontaktieren des Federated Authentication Service **default** an. Dies kann über die Optionen zur Konfiguration der Gruppenrichtlinie geändert werden.

Zum Erstellen einer neuen Zertifikatvorlage kopieren Sie die Vorlage "Citrix_SmartcardLogon" in der Microsoft-Zertifizierungsstellenkonsole, benennen Sie sie um (z. B. in "Citrix_SmartcardLogon2") und bearbeiten Sie sie nach Bedarf. Erstellen Sie mit einem Klick auf **Hinzufügen** eine neue Benutzerregel, die auf die neue Zertifikatvorlage verweist.

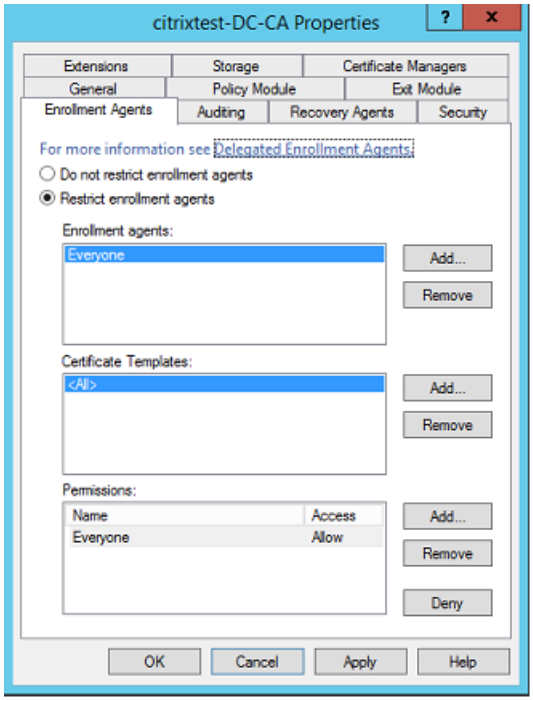
# Sicherheitsüberlegungen

Der Federated Authentication Service hat ein Registrierungsstellenzertifikat, mit dem er autonom Zertifikate für die Domänenbenutzer ausstellen kann. Es ist daher wichtig, eine Sicherheitsrichtlinie zum Schutz des FAS-Servers zu entwickeln und zu implementieren und die zugehörigen Berechtigungen einzuschränken.

**Delegierte Registrierungs-Agents**

Über die Microsoft-Zertifizierungsstelle können Sie festlegen, welche Vorlagen der FAS-Server verwenden kann, und die Zahl der Benutzer, denen der FAS-Server Zertifikate ausstellen kann, limitieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Citrix empfiehlt dringend, diese Optionen zu konfigurieren, damit der Federated Authentication Service nur den beabsichtigten Benutzern Zertifikate ausstellen kann. Es empfiehlt sich beispielsweise, eine Ausstellung von Zertifikaten für Benutzer in der Verwaltungsgruppe oder der Gruppe der geschützten Benutzer durch den Federated Authentication Service zu unterbinden.

### Konfigurieren der Zugriffssteuerungsliste

Wie im Abschnitt Konfigurieren von Benutzerrollen beschrieben, müssen Sie eine Liste von StoreFront-Servern konfigurieren, die als vertrauenswürdig gelten und bei der Ausstellung von Zertifikaten dem Federated Authentication Service Benutzeridentitäts-Assertions erstellen dürfen. Sie können außerdem festlegen, welchen Benutzern Zertifikate ausgestellt werden dürfen und bei welchen VDA-Maschinen sie sich authentifizieren können. Dies versteht sich zusätzlich zu den von Ihnen konfigurierten Active Directory- bzw. Zertifizierungsstellen-Standardsicherheitsfeatures.

### Firewalleinstellungen

Für die gesamte Kommunikation mit FAS-Servern werden gegenseitig authentifizierte Kerberos-Netzwerkverbindungen gemäß Windows Communication Foundation über Port 80 verwendet.

### Ereignisprotokollüberwachung

Der Federated Authentication Service und der VDA schreiben Informationen in das Windows-Ereignisprotokoll. Diese können zur Überwachung und Überprüfung verwendet werden. Der Abschnitt Ereignisprotokolle enthält eine Liste möglicher Ereignisprotokolleinträge.

### Hardwaresicherheitsmodule

Alle privaten Schlüssel, einschließlich der Schlüssel der vom Federated Authentication Service ausgestellten Zertifikate, werden als nicht exportierbare private Schlüssel vom Netzwerkdienstkonto gespeichert. Der Federated Authentication Service unterstützt die Verwendung eines kryptographischen Hardwaresicherheitsmoduls, sollte eine Sicherheitsrichtlinie dies erfordern.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Eine detaillierte Kryptographiekonfiguration ist über die Datei FederatedAuthenticationService.exe.config verfügbar. Diese Einstellungen gelten für die Ersterstellung privater Schlüssel. Daher können verschiedene Einstellungen für private Registrierungsstellenschlüssel (z. B. 4096 Bit, TPM-geschützt) und Laufzeit-Benutzerzertifikate verwendet werden.

| Parameter | Beschreibung |
|---|---|
| ProviderLegacyCsp | Bei Einstellung auf "true" verwendet der FAS die Microsoft CryptoAPI (CAPI). Andernfalls verwendet der FAS die Microsoft Cryptography Next Generation-API (CNG). |
| ProviderName | Name des CAPI- oder CNG-Anbieters, der verwendet werden soll. |
| ProviderType | Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation. |
| KeyProtection | Steuert das Flag "Exportable" privater Schlüssel. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers (Trusted Platform Module), wenn die Hardware dies unterstützt. |
| KeyLength | Schlüssellänge privater RSA-Schlüssel. Zulässige Werte sind 1024, 2048 und 4096 (Standard = 2048). |

# PowerShell SDK

Die Verwaltungskonsole des Verbundauthentifizierungsdiensts eignet sich für einfache Bereitstellungen, während die PowerShell erweiterte Optionen bietet. Wenn Sie mit Optionen arbeiten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, ausschließlich PowerShell für die Konfiguration zu verwenden.

Mit dem folgenden Befehl werden die PowerShell-Cmdlets hinzugefügt:

**Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1**

Verwenden Sie **Get-Help** <*Cmdlet-Name*>, um die Cmdlet-Hilfe anzuzeigen. Die folgende Tabelle enthält einige Befehle, wobei * für das standardmäßige PowerShell-Verb (New, Get, Set, Remove usw.) steht.

| Befehle | Übersicht |
|---|---|
| *-FasServer | Zum Auflisten und Umkonfigurieren der FAS-Server in der aktuellen Umgebung |
| *-FasAuthorizationCertificate | Zum Verwalten des Registrierungsstellenzertifikats |
| *-FasCertificateDefinition | Zum Steuern der Parameter, die vom FAS beim Generieren von Zertifikaten verwendet werden |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

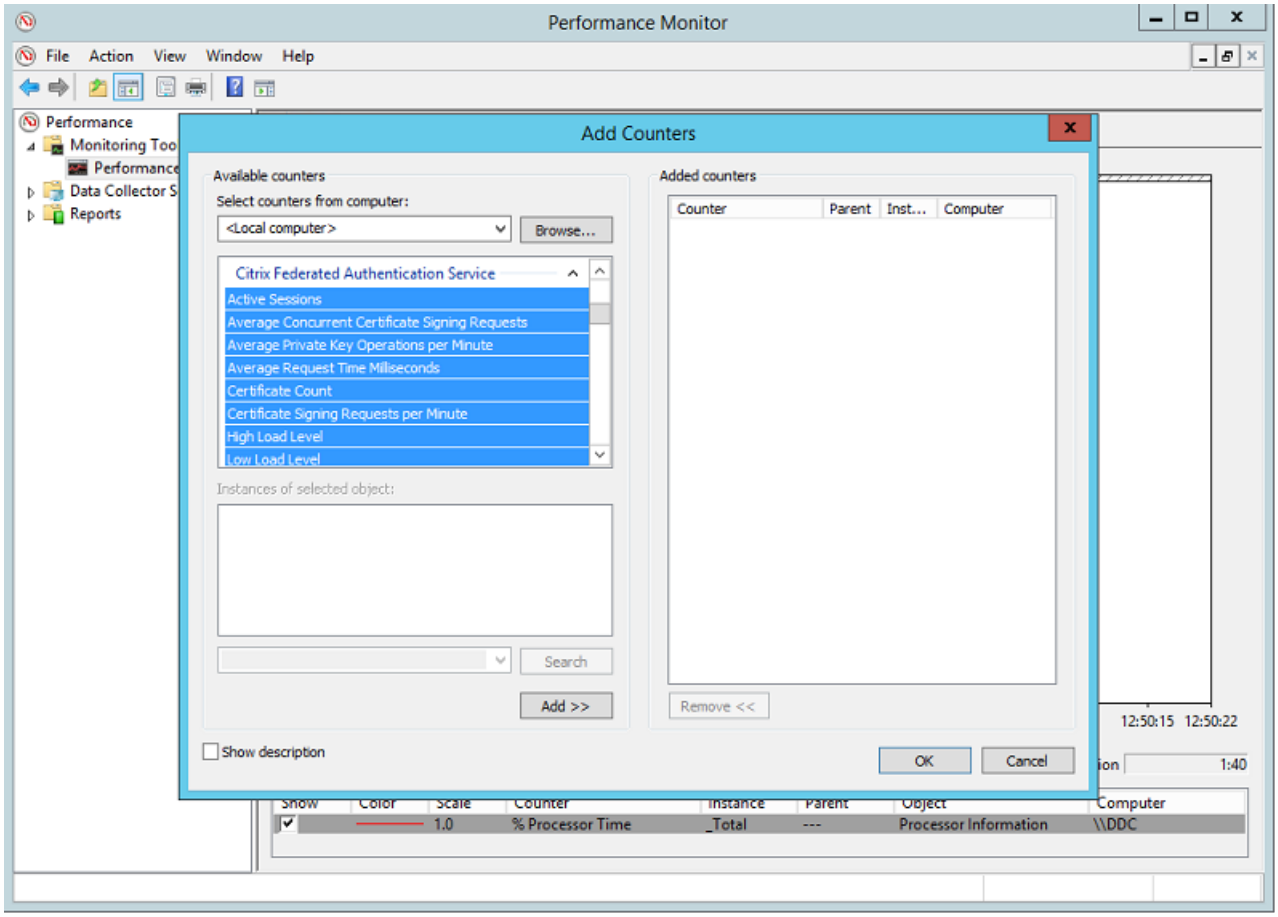
| | |
|---|---|
| *-FasRule | Zum Verwalten der für den Verbundauthentifizierungsdienst konfigurierten Benutzerregeln |
| *-FasUserCertificate | Zum Auflisten und Verwalten der vom Verbundauthentifizierungsdienst zwischengespeicherten Zertifikate |

PowerShell-Cmdlets können remote unter Angabe der Adresse eines FAS-Servers verwendet werden.

Sie können auch eine ZIP-Datei mit allen Cmdlet-Hilfedateien des PowerShell SDKs für FAS herunterladen. Weitere Informationen finden Sie im Artikel zum PowerShell SDK.

# Leistungsindikatoren

Der Federated Authentication Service enthält eine Reihe von Leistungsindikatoren zur Lastnachverfolgung.




In der folgenden Tabelle werden die Leistungsindikatoren aufgelistet. Die meisten Leistungsindikatoren sind gleitende Mittelwerte über fünf Minuten.

| Name | Beschreibung |
|---|---|
| | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Active Sessions | Anzahl der Verbindungen, die vom Federated Authentication Service nachverfolgt werden |
| Concurrent CSRs | Anzahl der gleichzeitig verarbeiteten Zertifikatanforderungen |
| Private Key ops | Anzahl der pro Minute für private Schlüssel durchgeführten Vorgänge |
| Request time | Länge der beim Generieren und Signieren eines Zertifikats verstrichenen Zeit |
| Certificate Count | Anzahl der im Federated Authentication Service zwischengespeicherten Zertifikate |
| CSR per minute | Anzahl der pro Minute verarbeiteten Zertifikatsignieranforderungen |
| Low/Medium/High | Schätzung der Last, die der Federated Authentication Service in Form von Zertifikatsignieranforderungen pro Minute übernehmen kann. Bei Überschreitung des Schwellenwerts für "High Load" können Sitzungsstarts fehlschlagen. |

# Ereignisprotokolle

Die folgenden Tabellen enthalten die vom Federated Authentication Service generierten Ereignisprotokolleinträge.

**Verwaltungsereignisse**

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

Diese Ereignisse werden bei einer Konfigurationsänderung des Federated Authentication Service-Servers protokolliert.

| Logcodes |
|---|
| [S001] ACCESS DENIED: User [{0}] is not a member of Administrators group |
| [S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}] |
| [S003] Administrator [{0}] setting Maintenance Mode to [{1}] |
| [S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}] |
| [S005] Administrator [{0}] de-authorizing CA [{1}] |
| [S006] Administrator [{0}] creating new Certificate Definition [{1}] |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| |
|---|
| [S007] Administrator [{0}] updating Certificate Definition [{1}] |
| [S008] Administrator [{0}] deleting Certificate Definition [{1}] |
| [S009] Administrator [{0}] creating new Role [{1}] |
| [S010] Administrator [{0}] updating Role [{1}] |
| [S011] Administrator [{0}] deleting Role [{1}] |
| [S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}] |
| [S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}] |

| Logcodes |
|---|
| [S401] Performing configuration upgrade -- [From version {0}][to version {1}] |
| [S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}] |

**Erstellen von Identitäts-Assertions [Federated Authentication Service]**

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem vertrauenswürdigen Server eine Assertion für eine Benutzeranmeldung erstellt wird.

| Logcodes |
|---|
| [S101] Server [{0}] is not authorized to assert identities in role [{1}] |
| [S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3}) |
| [S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3} |
| [S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}]) |
| [S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}] |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| |
|---|
| |
| [S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]] |
| [S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2} |
| [S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}]. |

**Bei Agieren als vertrauende Seite [Federated Authentication Service]**

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem VDA ein Benutzer angemeldet wird.

| Logcodes |
|---|
| [S201] Relying party [{0}] does not have access to a password. |
| [S202] Relying party [{0}] does not have access to a certificate. |
| [S203] Relying party [{0}] does not have access to the Logon CSP |
| [S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}] |
| [S205] Calling account [{0}] is not a relying party in role [{1}] |
| [S206] Calling account [{0}] is not a relying party |
| [S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}] |
| [S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}]. |

**Server für sitzungsinterne Zertifikate [Federated Authentication Service]**

Diese Ereignisse werden auf dem FAS-Server protokolliert, wenn ein Benutzer ein sitzungsinternes Zertifikat verwendet.

| Logcodes |
|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| |
|---|
| [S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card |
| [S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}] |
| [S303] User [{0}] does not match Virtual Smart Card [upn: {1}] |
| [S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}] |
| [S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}]. |

**Anmeldung [VDA]**

[Ereignisquelle: Citrix.Authentication.IdentityAssertion]

Diese Ereignisse werden bei der Anmeldung auf dem VDA protokolliert.

| Logcodes |
|---|
| [S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}] |
| [S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}] |
| [S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2} |
| [S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}] |
| [S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}] |
| [S106] Identity Assertion Logon. Logging in [Certificate: {0}] |
| [S107] Identity Assertion Logon failed. [Exception: {1}{2}] |
| [S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}] |

**Sitzungsinterne Zertifikate [VDA]**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Diese Ereignisse werden auf dem VDA protokolliert, wenn ein Benutzer versucht, ein sitzungsinternes Zertifikat zu verwenden.

| Logcodes |
| --- |
| [S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}] |
| [S202] Virtual Smart Card Subsystem. No smart cards available in session {0} |
| [S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}] |
| [S204] Virtual Smart Card Subsystem. Smart card support disabled. |

**Zertifikatanforderung und Generierungscodes [Federated Authentication Service]**

Ereignisquelle: Citrix.TrustFabric]

Diese Detailereignisse werden protokolliert, wenn der FAS-Server kryptographische Vorgänge auf Protokollebene durchführt.

| Logcodes |
| --- |
| [S0001]TrustArea::TrustArea: Installed certificate chain |
| [S0002]TrustArea::Join: Callback has authorized an untrusted certificate |
| [S0003]TrustArea::Join: Joining to a trusted server |
| [S0004]TrustArea::Maintain: Renewed certificate |
| [S0005]TrustArea::Maintain: Retrieved new certificate chain |
| [S0006]TrustArea::Export: Exporting private key |
| [S0007]TrustArea::Import: Importing Trust Area |
| [S0008]TrustArea::Leave: Leaving Trust Area |
| [S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| |
|---|
| [S0010]CertificateVerification: Installing new trusted certificate |
| [S0011]CertificateVerification: Uninstalling expired trusted certificate |
| [S0012]TrustFabricHttpClient: Attempting single sign-on to {0} |
| [S0013]TrustFabricHttpClient: Explicit credentials entered for {0} |
| [S0014]Pkcs10Request::Create: Created PKCS10 request |
| [S0015]Pkcs10Request::Renew: Created PKCS10 request |
| [S0016]PrivateKey::Create |
| [S0017]PrivateKey::Delete |
| [S0018]TrustArea::TrustArea: Waiting for Approval |
| [S0019]TrustArea::Join: Delayed Join |
| [S0020]TrustArea::Join: Delayed Join |
| [S0021]TrustArea::Maintain: Installed certificate chain |

| Logcodes |
|---|
| [S0101]TrustAreaServer::Create root certificate |
| [S0102]TrustAreaServer::Subordinate: Join succeeded |
| [S0103]TrustAreaServer::PeerJoin: Join succeeded |
| [S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0} |
| [S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0} |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| |
|---|
| [S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0} |
| [S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL |
| [S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0} |
| [S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0} |
| [S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval |
| [S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused |
| [S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate |
| [S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval |
| [S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0} |
| [S0121]NativeCertificateAuthority::SubmitCertificateRequest Error |
| [S0122]NativeCertificateAuthority::RootCARollover New root certificate |
| [S0123]NativeCertificateAuthority::ReissueCertificate New certificate |
| [S0124]NativeCertificateAuthority::RevokeCertificate |
| [S0125]NativeCertificateAuthority::PublishCRL |

# Verwandte Informationen

- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Übersicht über die Architekturen des Verbundauthentifizierungsdiensts

Jul 13, 2016

# Einführung

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eine Citrix Komponente zur Integration in die Active Directory-Zertifizierungsstelle (ZS), die eine nahtlose Authentifizierung der Benutzer innerhalb einer Citrix Umgebung ermöglicht. In diesem Dokument werden die verschiedenen Authentifizierungsarchitekturen beschrieben, die für diverse Bereitstellungen geeignet sein können.

Wenn der FAS aktiviert ist, delegiert er die Entscheidung über die Benutzerauthentifizierung an vertrauenswürdige StoreFront-Server. StoreFront besitzt umfassende integrierte Authentifizierungsoptionen, die auf modernen Internettechnologien aufbauen. Es kann problemlos mit dem StoreFront-SDK oder IIS-Plug-Ins anderer Hersteller erweitert werden. Das grundlegende Designziel besteht darin, dass jede Technologie zur Authentifizierung von Benutzern bei einer Website nun auch für die Anmeldung bei einer Citrix XenApp- oder XenDesktop-Bereitstellung verwendet werden kann.

In diesem Dokument werden die Beispiele einiger Bereitstellungsarchitekturen in der Reihenfolge zunehmender Komplexität vorgestellt.

- Interne Bereitstellung
- NetScaler Gateway-Bereitstellung
- AD FS SAML
- B2B-Kontozuordnung
- Einbindung in Azure AD unter Windows 10

Das Dokument enthält außerdem Links zu verwandten FAS-Artikeln. Für alle Architekturen gilt der Artikel Verbundauthentifizierungsdienst als primäre Referenz für das Einrichten des FAS.

### Funktionsweise

Der FAS kann für Active Directory-Benutzer, die von StoreFront authentifiziert werden, automatisch Zertifikate der Smartcardklasse ausstellen. Dabei werden ähnliche APIs verwendet, wie bei Tools zum Bereitstellen physischer Smartcards.

Wenn ein Benutzer an einen Citrix XenApp- oder XenDesktop-VDA vermittelt wird, wird das Zertifikat der Maschine angehängt und die Anmeldung von der Windows-Domäne als normale Smartcard-Authentifizierung behandelt.

# Interne Bereitstellung

Der FAS ermöglicht die sichere Authentifizierung der Benutzer bei StoreFront mit einer Reihe von Authentifizierungsoptionen (einschließlich Kerberos-Single Sign-On) und die Verbindung mit einer vollauthentifizierten Citrix HDX-Sitzung.

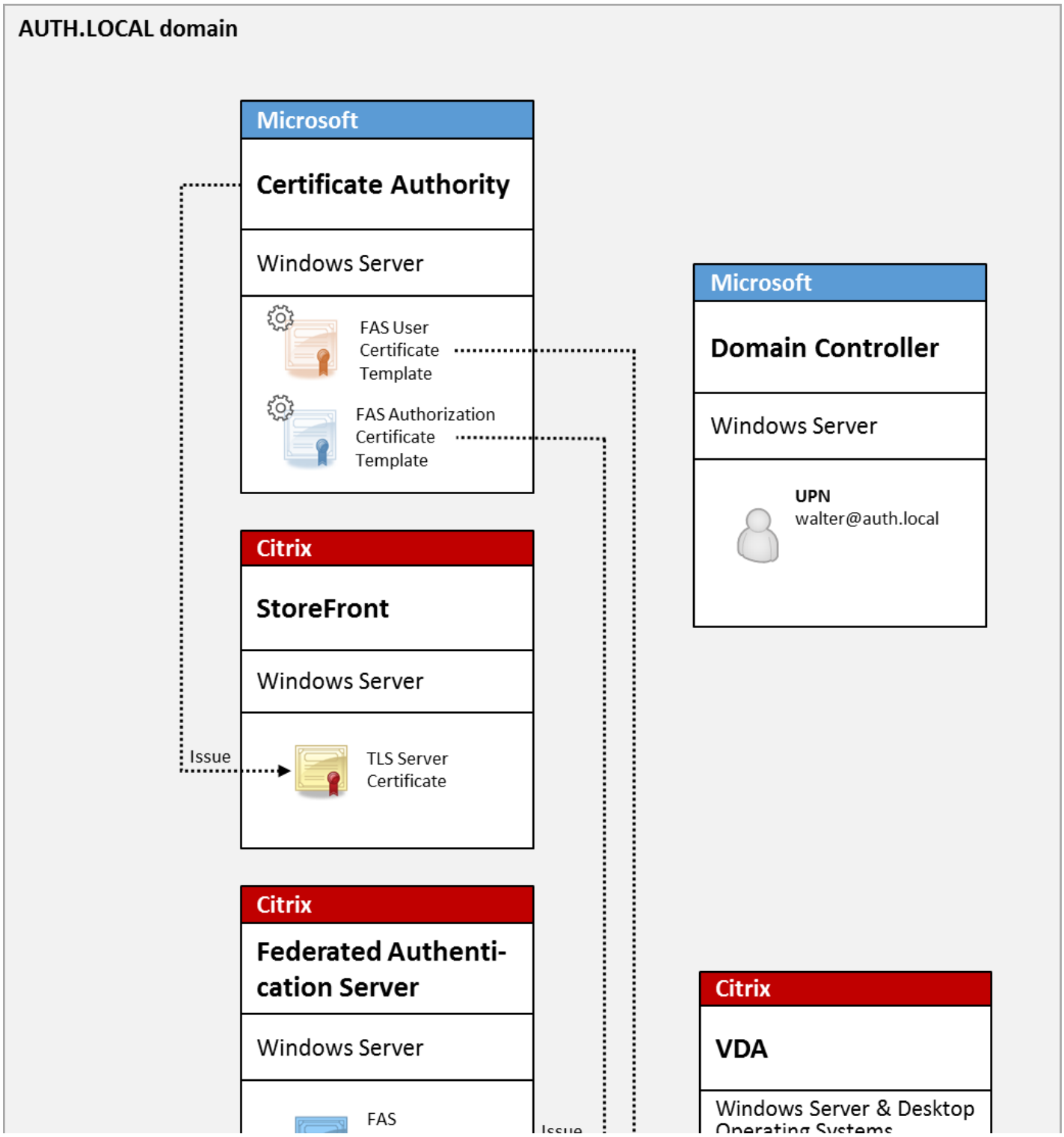
Dies ermöglicht die Windows-Authentifizierung ohne Aufforderungen zur Eingabe von Anmeldeinformationen oder Smartcard-PINs und ohne Verwaltung gespeicherter Kennwörter wie beim Single Sign-On-Dienst. Der Service kann die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Anmeldefeatures der eingeschränkten Kerberos-Delegierung älterer Versionen von XenApp ersetzen.

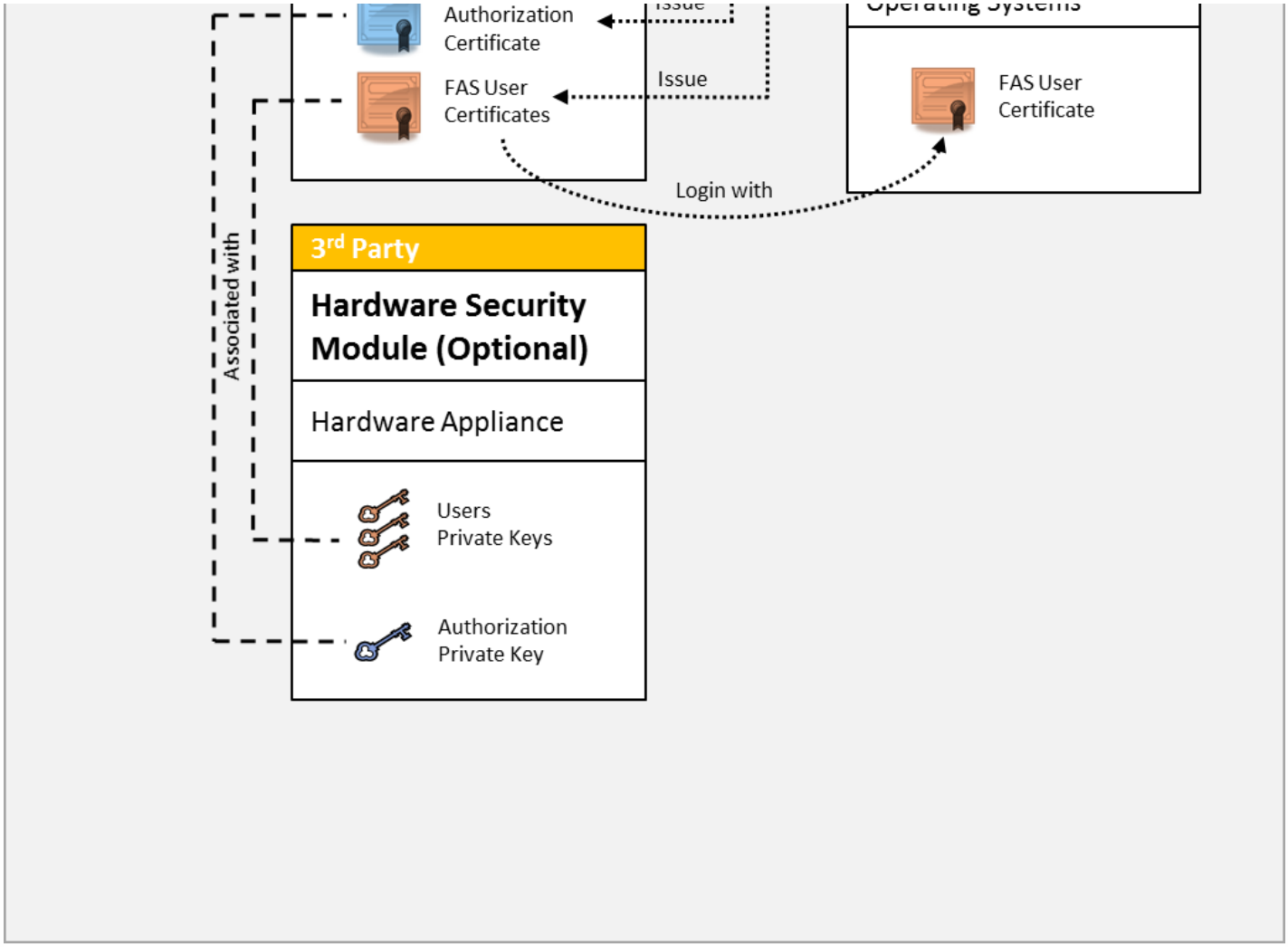
Alle Benutzer haben Zugriff auf Public Key-Infrastruktur-Zertifikate in ihrer Sitzung, unabhängig davon, ob sie sich bei Endpunktgeräten mit einer Smartcard angemeldet haben. Dies ermöglicht eine reibungslose Migration zur zweistufigen Authentifizierung, und zwar selbst bei Smartphones, Tablets und ähnlichen Geräten ohne Smartcardleser.

Bei dieser Bereitstellung gibt es einen neuen Server, auf dem der FAS ausgeführt wird und der Zertifikate der Smartcardklasse für Benutzer ausstellen darf. Die Zertifikate werden dann zur Anmeldung bei Benutzersitzungen in einer Citrix HDX-Umgebung verwendet, die wie eine klassische Smartcard-Anmeldung verarbeitet wird.





© 1999-2017 Citrix Systems, Inc. All rights reserved.




Die XenApp- oder XenDesktop-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie in dem Abschnitt zum Ausstellen von Domänencontrollerzertifikaten in CTX206156.)

Verwandte Informationen

- Schlüssel können in einem Hardwaresicherheitsmodul (HSM) oder einem integrierten Trusted Platform Module (TPM) gespeichert werden. Weitere Informationen finden Sie in dem Artikel Schutz durch private Schlüssel beim Verbundauthentifizierungsdienst.
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

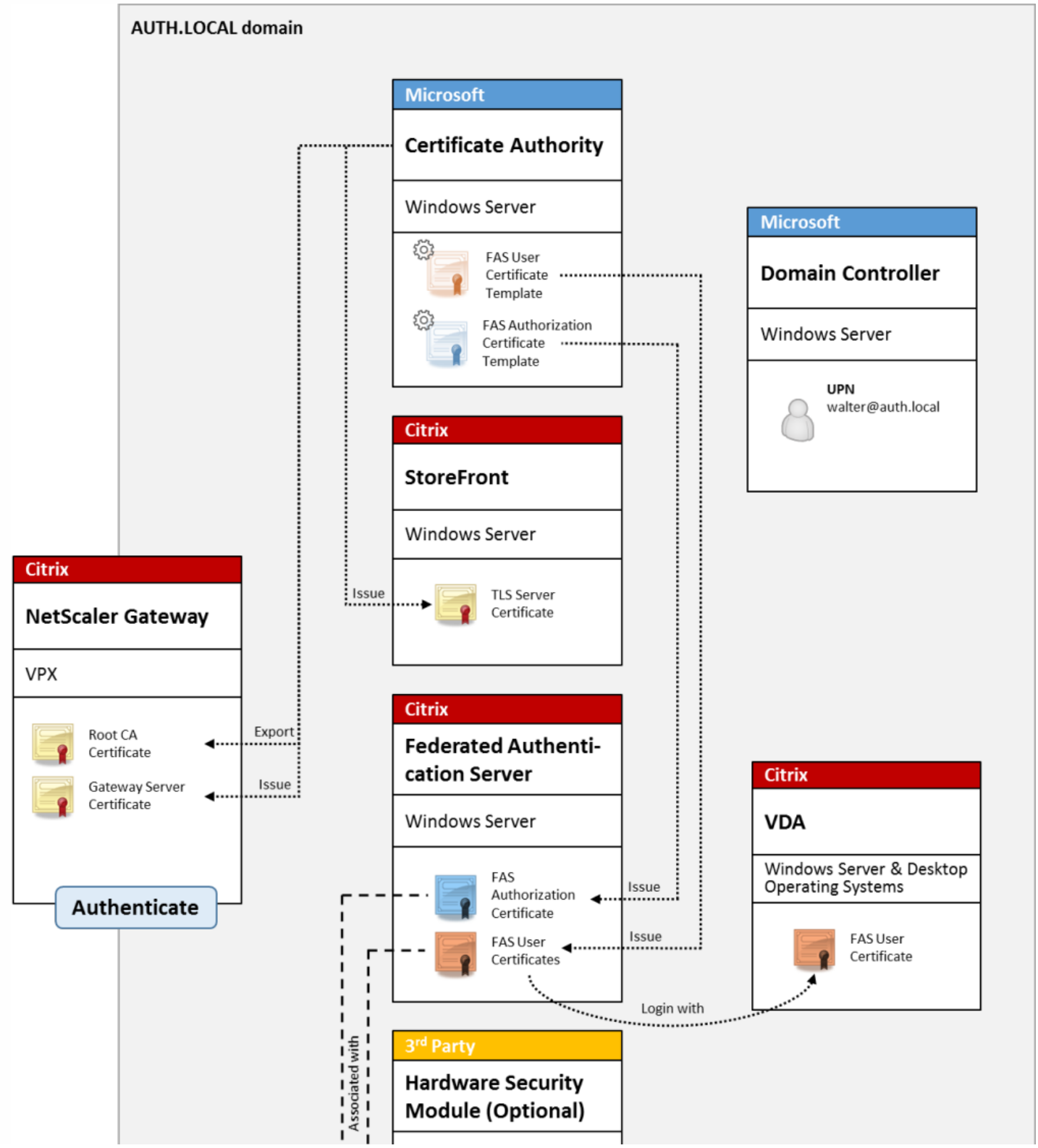
# NetScaler Gateway-Bereitstellung

Die NetScaler-Bereitstellung ähnelt der internen Bereitstellung, wobei zusätzlich ein mit StoreFront gekoppeltes Citrix NetScaler Gateway verwendet wird und die primäre Authentifizierung in NetScaler erfolgt. Citrix NetScaler bietet


© 1999-2017 Citrix Systems, Inc. All rights reserved.

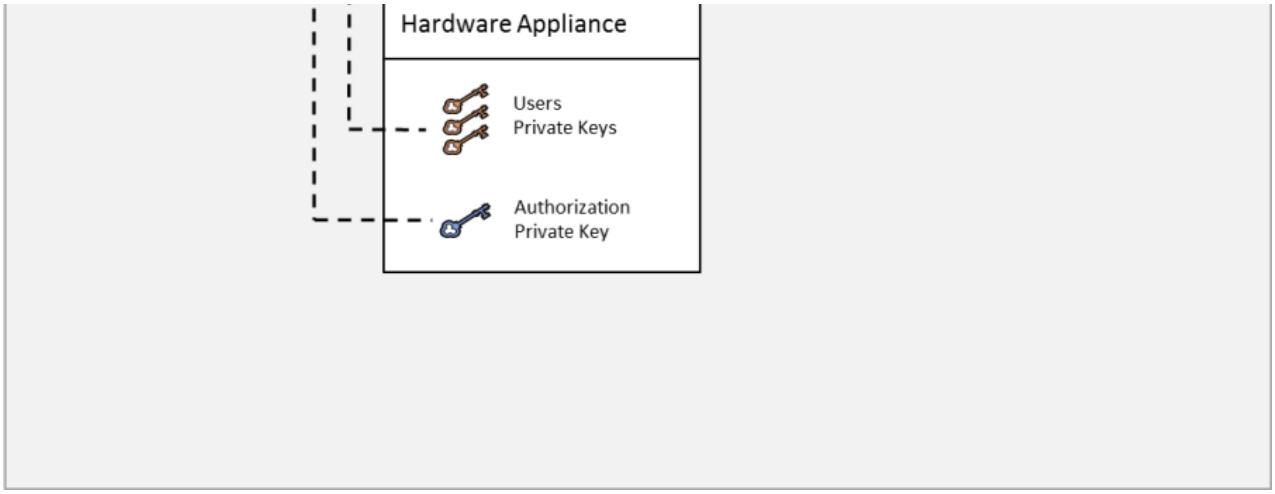
intelligente Optionen für Authentifizierung und Autorisierung, mit denen der Remotezugriff auf die Websites eines Unternehmens gesichert werden kann.

Diese Bereitstellung kann verwendet werden, um mehrere PIN-Eingabeaufforderungen zu vermeiden, wie sie bei der Authentifizierung bei NetScaler und anschließender Anmeldung bei einer Benutzersitzung auftreten. Außerdem können erweiterte NetScaler-Authentifizierungstechnologien ohne zusätzliche Active Directory-Kennwörter oder Smartcards genutzt werden.





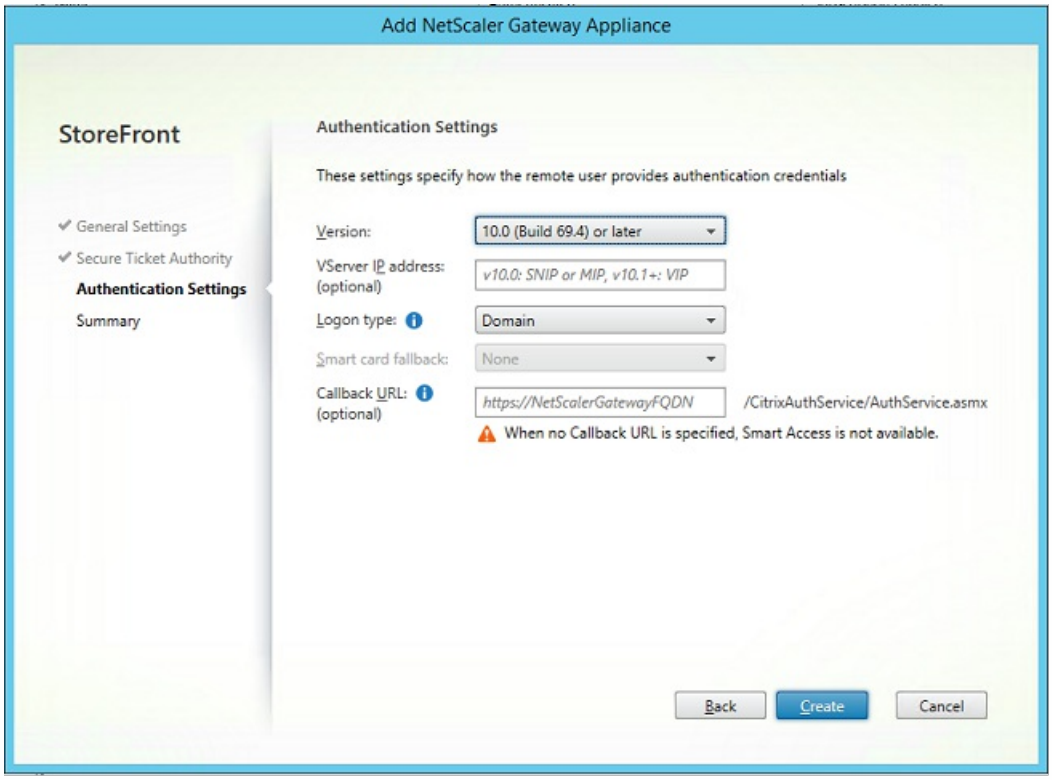
© 1999-2017 Citrix Systems, Inc. All rights reserved.




Die XenApp- oder XenDesktop-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie in dem Abschnitt zum Ausstellen von Domänencontrollerzertifikaten in CTX206156.)

Bei der Konfiguration von NetScaler als primäres Authentifizierungssystem müssen alle Verbindungen zwischen NetScaler und StoreFront mit TLS geschützt werden. Sorgen Sie vor allem dafür, dass die Callback-URL richtig auf den NetScaler-Server zeigt, denn sie kann zur Authentifizierung des NetScaler-Servers in dieser Bereitstellung verwendet werden.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

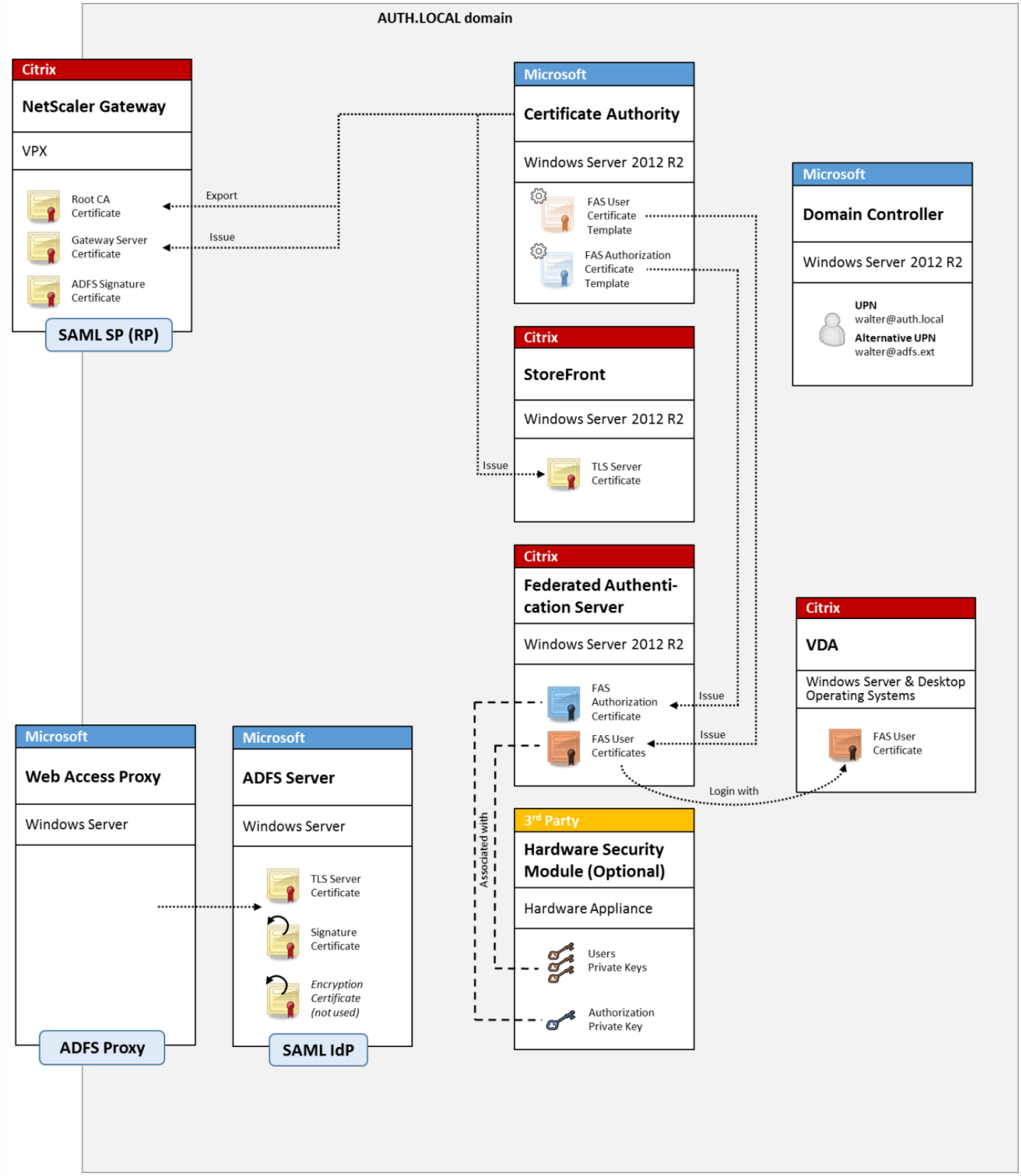
Verwandte Informationen

- Informationen zum Konfigurieren von NetScaler Gateway finden Sie unter How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6.
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

# AD FS SAML-Bereitstellung

Eine wichtige NetScaler-Authentifizierungstechnologie ermöglicht die Integration in Microsoft AD FS zur Verwendung als SAML-Identitätsanbieter (IdP). Eine SAML-Assertion ist ein kryptografisch signierter XML-Block, der von einem vertrauenswürdigen IdP ausgestellt wird und einen Benutzer zur Anmeldung bei einem Computersystem autorisiert. Der FAS-Server gestattet die Delegation der Authentifizierung eines Benutzers an den Microsoft AD FS-Server (oder einen anderen SAML-fähigen IdP).


© 1999-2017 Citrix Systems, Inc. All rights reserved.




AD FS wird häufig zur sicheren Authentifizierung von Benutzern bei Unternehmensressourcen remote über das Internet verwendet (z. B. bei einer Office 365-Integration).

Verwandte Informationen

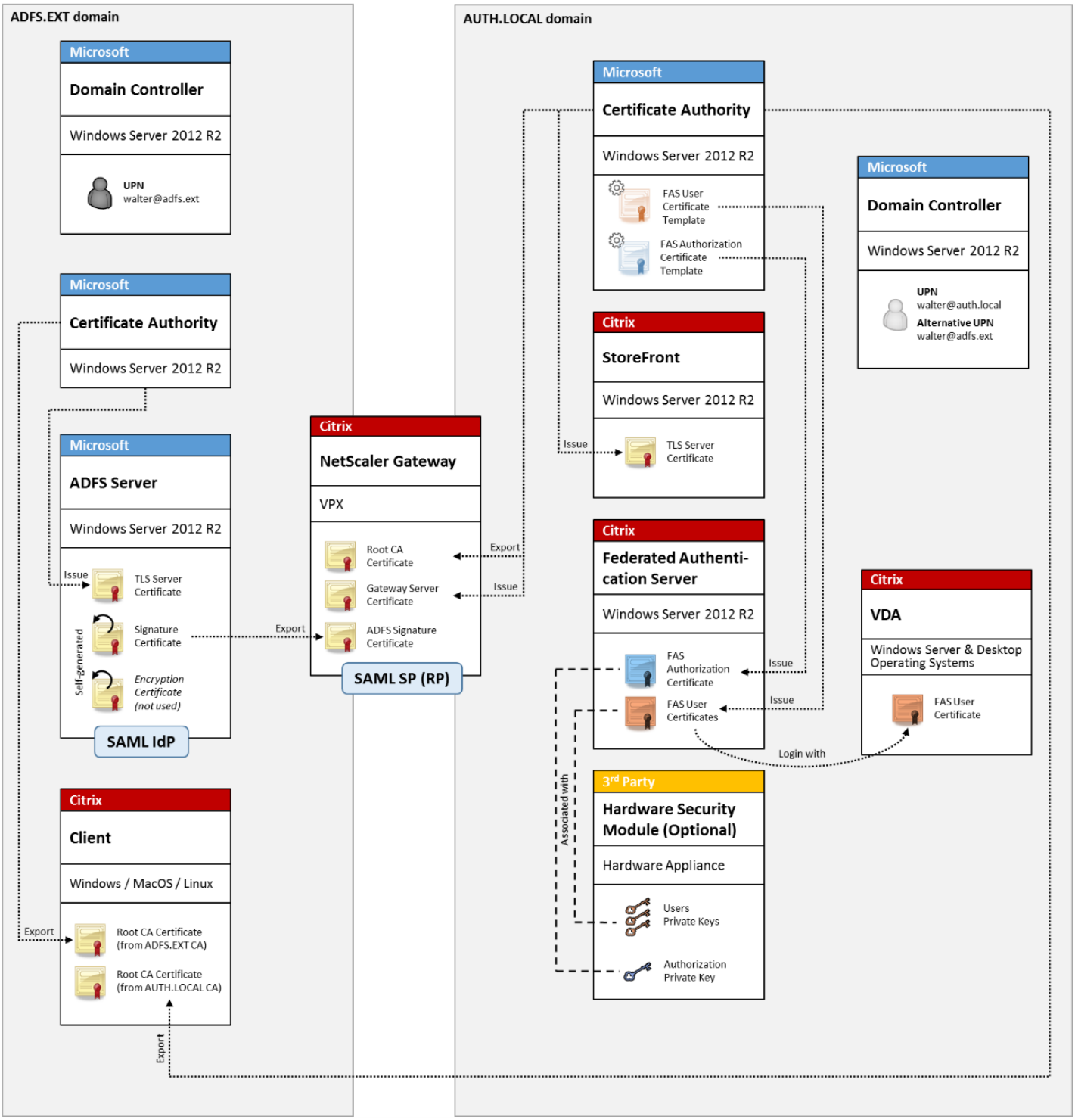

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Der Artikel AD FS-Bereitstellung des Verbundauthentifizierungsdiensts enthält detaillierte Informationen.
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.
- Der Abschnitt NetScaler Gateway-Bereitstellung des Artikels enthält Hinweise zur Konfiguration.

# B2B-Kontozuordnung

Wenn zwei Unternehmen ihre Computersysteme gemeinsam verwenden möchten, wird häufig ein Active Directory-Verbunddienste-Server (AD FS) mit einer Vertrauensstellung eingerichtet. Dadurch können Benutzer in einem Unternehmen sich nahtlos bei dem Active Directory (AD) des zweiten authentifizieren. Die Benutzer verwenden bei der Anmeldung die Anmeldeinformationen ihres eigenen Unternehmens, die von AD FS automatisch einem Schattenkonto in der AD-Umgebung des zweiten Unternehmens zugewiesen wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Verwandte Informationen

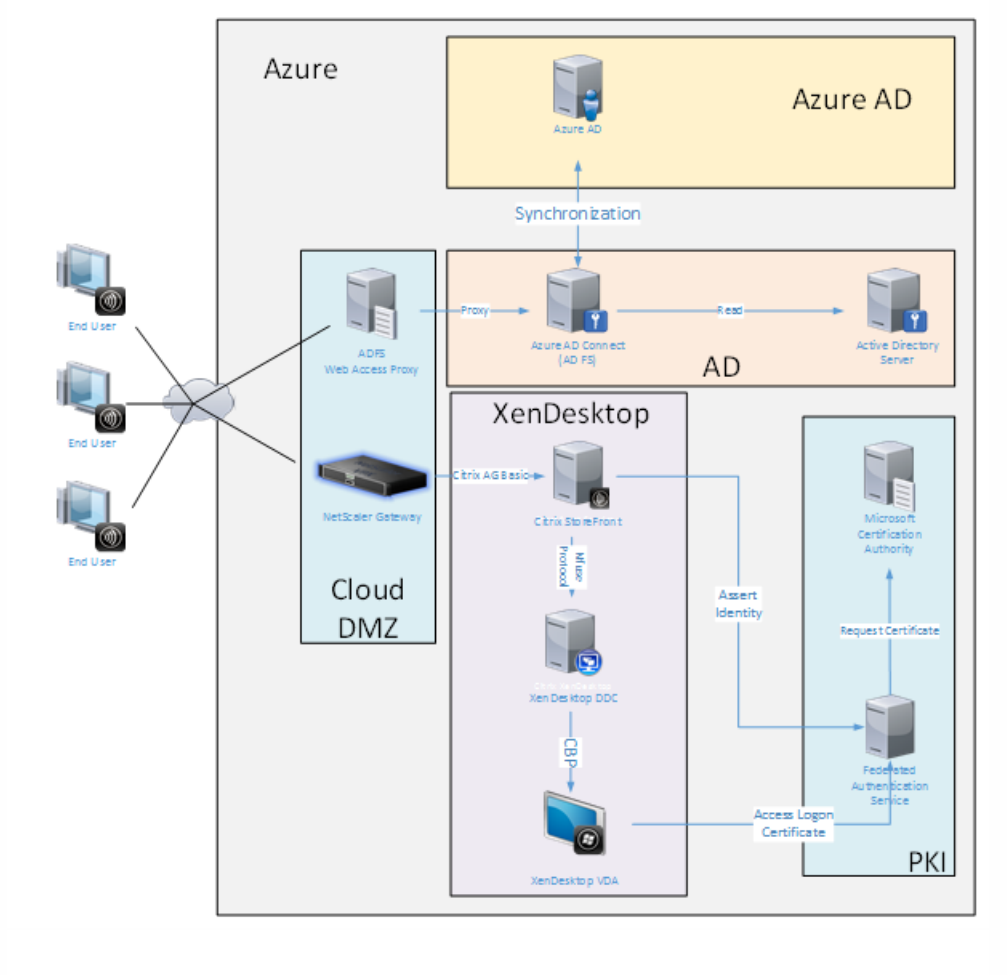
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

# Einbindung in Azure AD unter Windows 10

Mit Windows 10 wurde das Konzept der AD-Einbindung eingeführt, welches dem herkömmlichen Beitritt zu einer Windows-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Domäne entspricht, jedoch auf Verbindungen über das Internet abzielt. Es funktioniert gut mit Laptops und Tablets. Genau wie der herkömmliche Windows-Domänenbeitritt bietet Azure AD Funktionen, die Single Sign-On-Modelle für Unternehmenswebsites und -ressourcen zulassen. Diese sind allesamt Internet-fähig und können daher an jedem Standort mit Internetverbindung und nicht nur im Unternehmens-LAN verwendet werden.




Diese Bereitstellung ist ein Beispiel, bei dem es das Konzept "Endbenutzer im Büro" praktisch nicht gibt. Laptops werden vollständig über das Internet mit modernen Azure AD-Features registriert und authentifiziert.

Die Infrastruktur dieser Bereitstellung kann überall dort ausgeführt werden, wo eine IP-Adresse verfügbar ist: lokal, bei einem Hostinganbieter, in Azure oder in einer anderen Cloud. Die Synchronisierung von Azure AD Connect stellt automatisch eine Verbindung mit Azure AD her. In der Beispielabbildung werden der Einfachheit halber VMs verwendet.

Verwandte Informationen

- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.
- Der Artikel Integration des Verbundauthentifizierungsdiensts in Azure Active Directory enthält detaillierte Informationen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# AD FS-Bereitstellung des Verbundauthentifizierungsdiensts

Jul 13, 2016

## Einführung

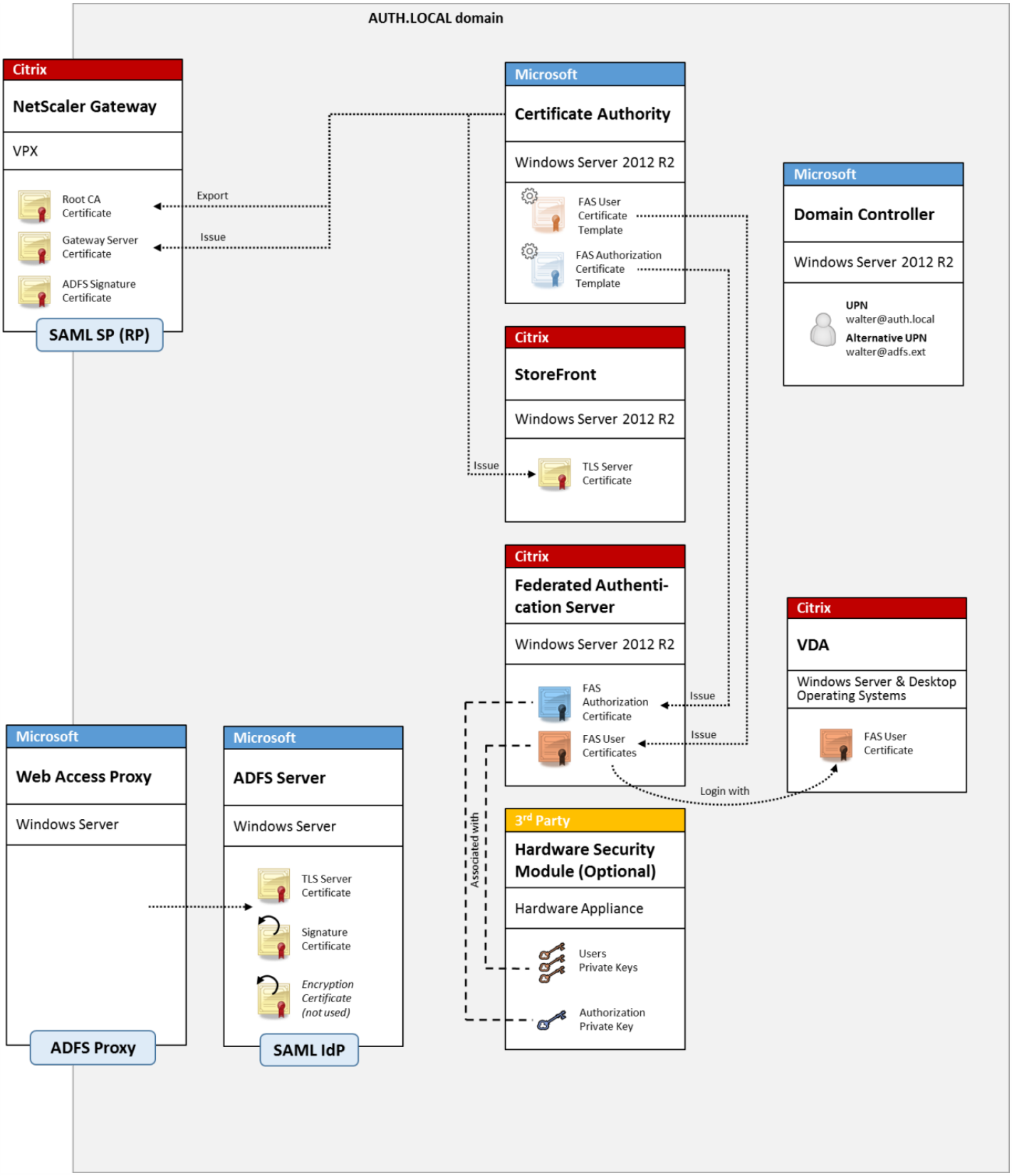
In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Microsoft Active Directory-Verbunddienste integrieren.

In vielen Organisationen wird AD FS zum Verwalten des sicheren Benutzerzugriffs auf Websites verwendet, die einen einzelnen Authentifizierungspunkt erfordern. Wenn beispielsweise Mitarbeitern zusätzliche Inhalte und Downloads zur Verfügung stehen, müssen diese durch standardmäßige Windows-Anmeldeinformationen geschützt werden.

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ermöglicht zudem die Integration von Citrix NetScaler und Citrix StoreFront in das AD FS-Anmeldesystem und vereinfacht so die Anmeldung für das Personal.

Bei einer solchen Bereitstellung wird NetScaler als vertrauende Seite für Microsoft AD FS integriert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Übersicht über SAML


© 1999-2017 Citrix Systems, Inc. All rights reserved.

SAML (Security Assertion Markup Language) ist eine einfaches System für die Webbrowser-Anmeldung, durch das eine Umleitung auf eine Anmeldeseite vorgenommen wird. Die Konfiguration umfasst folgende Elemente:

**Umleitungs-URL (URL des Single Sign-On-Diensts)**

Wenn NetScaler erkennt, dass ein Benutzer authentifiziert werden muss, weist es den Webbrowser zur Durchführung eines HTTP POST an eine SAML-Anmeldeseite auf dem AD FS-Server an. Das ist normalerweise eine https://-Adresse im Format https://adfs.mycompany.com/adfs/ls.

Der Webseiten-POST umfasst weitere Informationen, darunter eine Rückleitungsadresse, an die der Benutzer nach der Anmeldung zurückgeleitet wird.

**Bezeichner (Ausstellername/EntityID)**

Die EntityID ist ein eindeutiger Bezeichner, der von NetScaler in den POST-Daten an AD FS verwendet wird. Durch ihn wird AD FS darüber informiert, bei welchem Dienst der Benutzer versucht, sich anzumelden und welche Authentifizierungsrichtlinien anzuwenden sind. Wenn eine SAML-Authentifizierungs-XML ausgestellt wird, kann diese nur für die Anmeldung bei dem durch die EntityID bezeichneten Dienst verwendet werden.

Normalerweise ist die EntityID die URL der Anmeldeseite des NetScaler-Servers. Es kann jedoch eine beliebige andere EntityID verwendet werden, vorausgesetzt NetScaler und AD FS interpretieren sie beide als gültig: https://ns.mycompany.com/application/logonpage.

**Rückleitungsadresse (Antwort-URL)**

Wenn die Authentifizierung erfolgreich ist, weist AD FS den Webbrowser des Benutzers an, einen POST einer SAML-Authentifizierungs-XML an eine der Antwort-URLs vorzunehmen, die für die EntityID konfiguriert wurden. Das ist normalerweise eine https://-Adresse auf dem ursprünglichen NetScaler-Server im Format: https://ns.mycompany.com/cgi/samlauth.

Sind mehrere Antwort-URLs konfiguriert, kann NetScaler eine aus dem ursprünglichen POST an AD FS wählen.

**Signaturzertifikat (IDP-Zertifikat)**

SAML-Authentifizierungs-XML-Blobs werden von AD FS kryptografisch mit seinem privaten Schlüssel signiert. Zur Überprüfung der Signatur muss NetScaler zur Prüfung solcher Signaturen mit dem öffentlichen Schlüssel in der Zertifikatdatei konfiguriert sein. Die Zertifikatdatei ist normalerweise eine vom AD FS-Server erhaltene Textdatei.

**URL für Single Sign-Out (URL für einmaliges Abmelden)**

AD FS und NetScaler unterstützen ein zentrales Abmeldesystem. Das ist eine URL, die von NetScaler regelmäßig abgefragt wird, um zu prüfen, ob das SAML-Authentifizierungs-XML-Blob immer noch die aktuell angemeldete Sitzung repräsentiert.

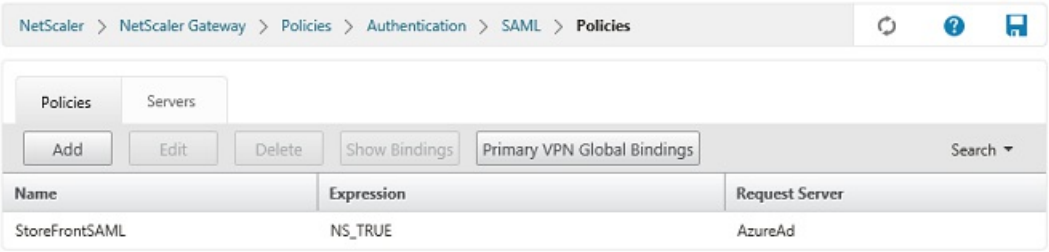
Dies ist ein optionales Feature, das nicht konfiguriert werden muss. Es ist normalerweise eine https://-Adresse im Format https://adfs.mycompany.com/adfs/logout. (Die Adresse darf nicht mit der URL für die einmalige Anmeldung identisch sein.)

# Konfiguration

Im Bereich NetScaler Gateway-Bereitstellung des Artikels Übersicht über die Architekturen des Verbundauthentifizierungsdiensts wird beschrieben, wie NetScaler Gateway mit dem NetScaler-Setupassistenten von

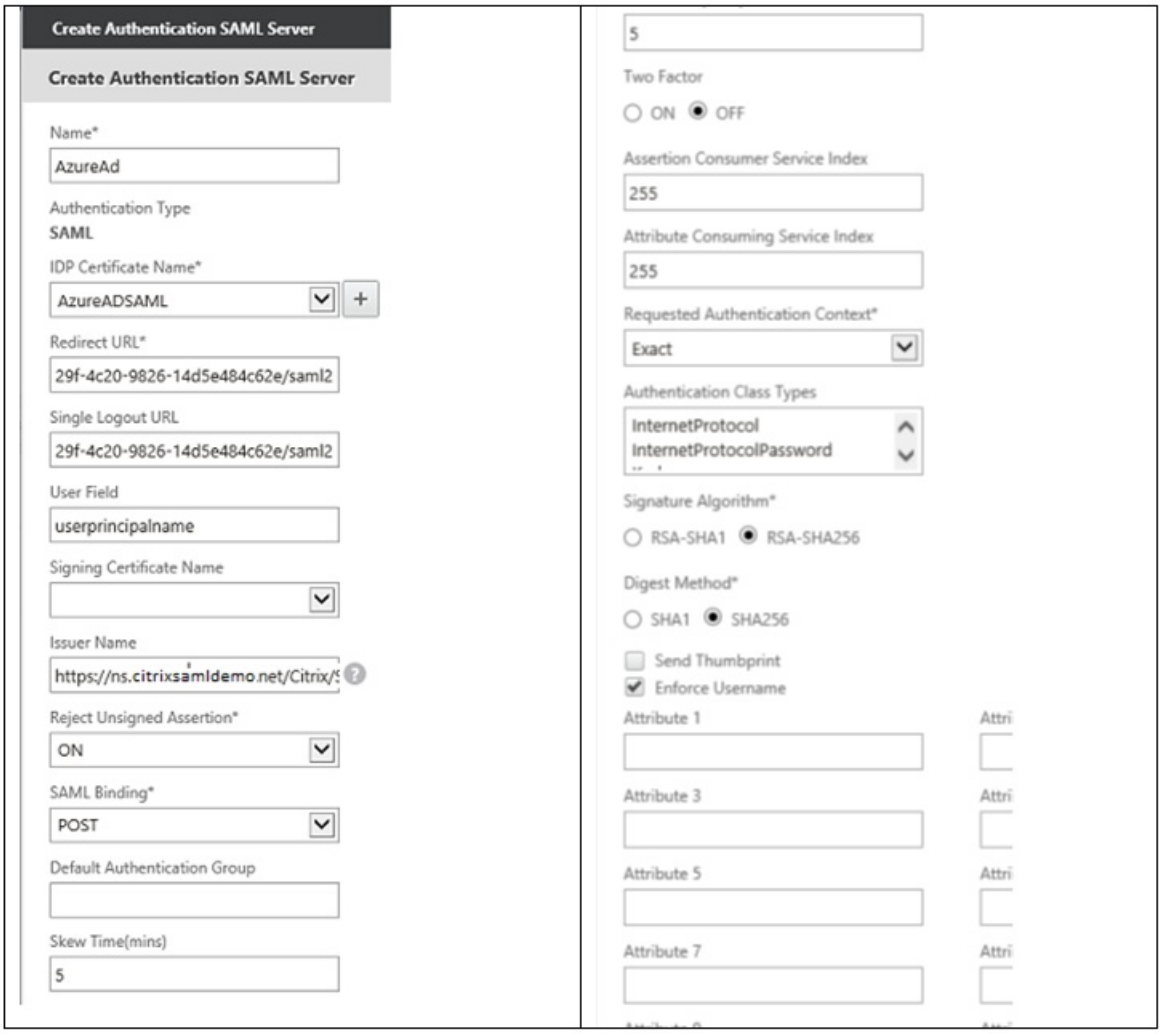
 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

XenApp und XenDesktop für die Standard-LDAP-Authentifizierungsoptionen konfiguriert wird. Nach diesem Arbeitsgang können Sie eine neue Authentifizierungsrichtlinie in NetScaler für die SAML-Authentifizierung erstellen. Diese kann dann die von dem NetScaler-Setupassistenten verwendete Standard-LDAP-Richtlinie ersetzen.




### Ausfüllen der SAML-Richtlinie

Konfigurieren Sie den neuen SAML-IdP-Server mit den zuvor der AD FS-Verwaltungskonsole entnommenen Informationen. Wenn diese Richtlinie angewendet wird, leitet NetScaler Benutzer zur Anmeldung an AD FS um und akzeptiert von AD FS signierte SAML-Authentifizierungs-XML-Blöcke.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Integration des Verbundauthentifizierungsdiensts in Azure Active Directory

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Architektur
- Erstellen einer DNS-Zone
- Erstellen eines Clouddiensts
- Erstellen virtueller Windows-Maschinen
- Konfigurieren eines internen DNS
- Konfigurieren einer externen DNS-Adresse
- Konfigurieren von Sicherheitsgruppen
- Erstellen eines AD FS-Zertifikats
- Einrichten von Azure Active Directory
- Aktivieren der Azure AD-Einbindung
- Installieren von XenApp oder XenDesktop
- Konfigurieren einer neuen Azure-Anwendung für das Single Sign-On bei StoreFront
- Installieren und Konfigurieren von NetScaler Gateway
- Konfigurieren der StoreFront-Adresse
- Aktivieren der Unterstützung für die NetScaler-SAML-Authentifizierung
- Überprüfen des Gesamtsystems
- Anhang

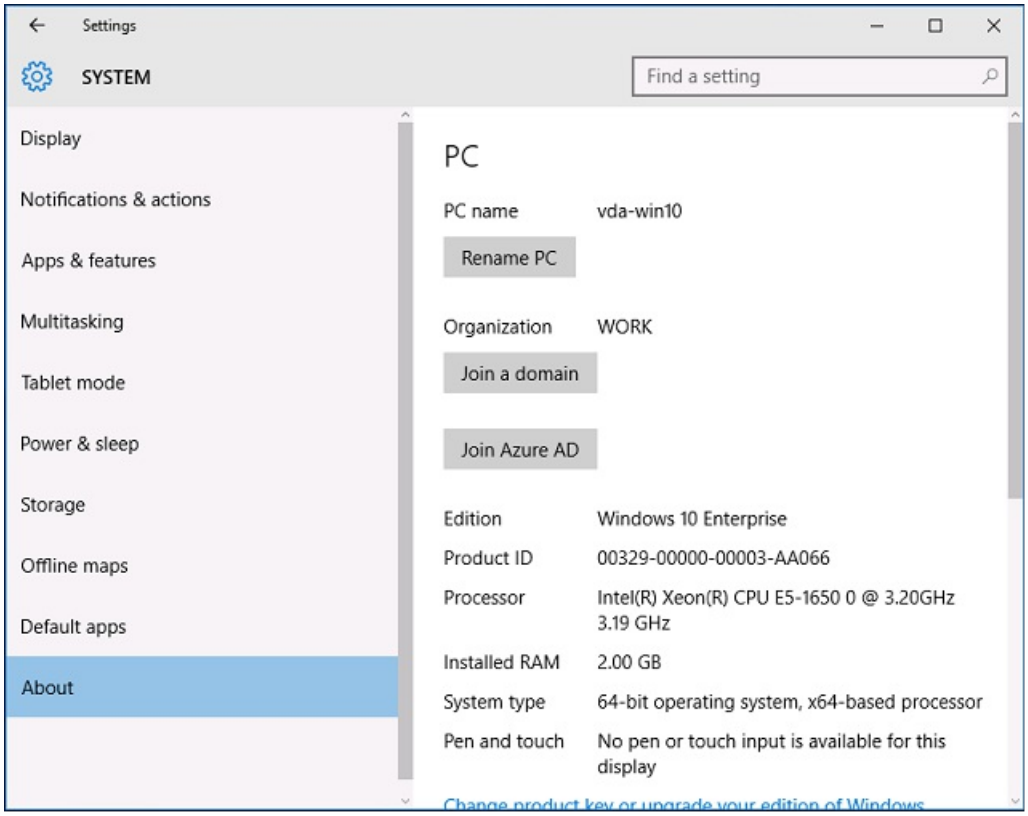

# Einführung

In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Azure Active Directory unter Windows 10 integrieren.

Azure Active Directory wurde mit Windows 10 eingeführt und repräsentiert ein neues Modell für den Domänenbeitritt, bei dem Laptops im Roamingbetrieb über das Internet einer Unternehmensdomäne für Verwaltungszwecke und zum Single Sign-On beitreten können.

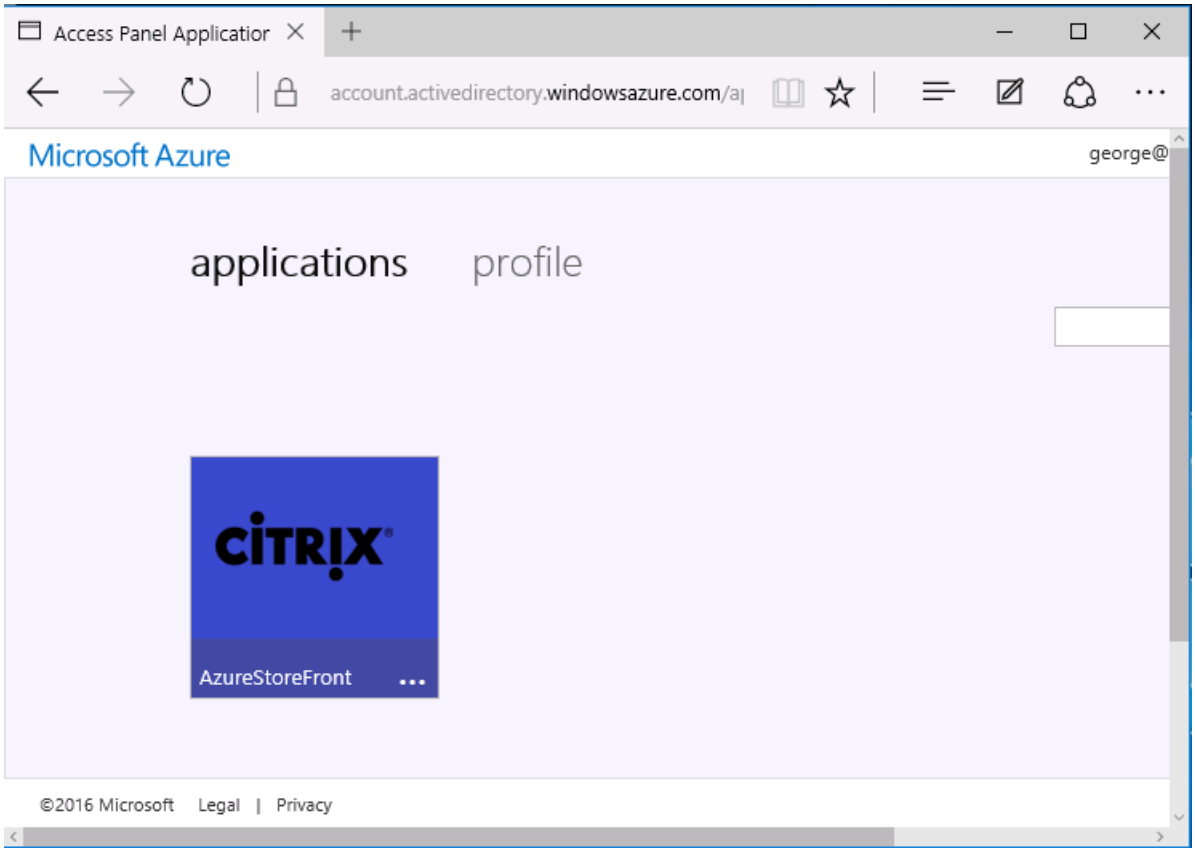
Die hier vorgestellte Beispielbereitstellung ist ein System, bei dem die IT neuen Benutzern eine Unternehmens-E-Mail-Adresse und einen Registrierungscode für ihre privaten Windows 10-Laptops zuteilt. Die Benutzer greifen auf diesen Code über die Option "System > Info > Azure AD beitreten" im Bereich **Einstellungen** zu.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Nach der Registrierung eines Laptops führt der Microsoft Edge-Webbrowser automatisch die Anmeldung bei Unternehmenswebsites und veröffentlichten Citrix Anwendungen über die Azure-SaaS-Anwendungswebsite durch, die auch andere Azure-Anwendungen, wie Office 365, bietet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

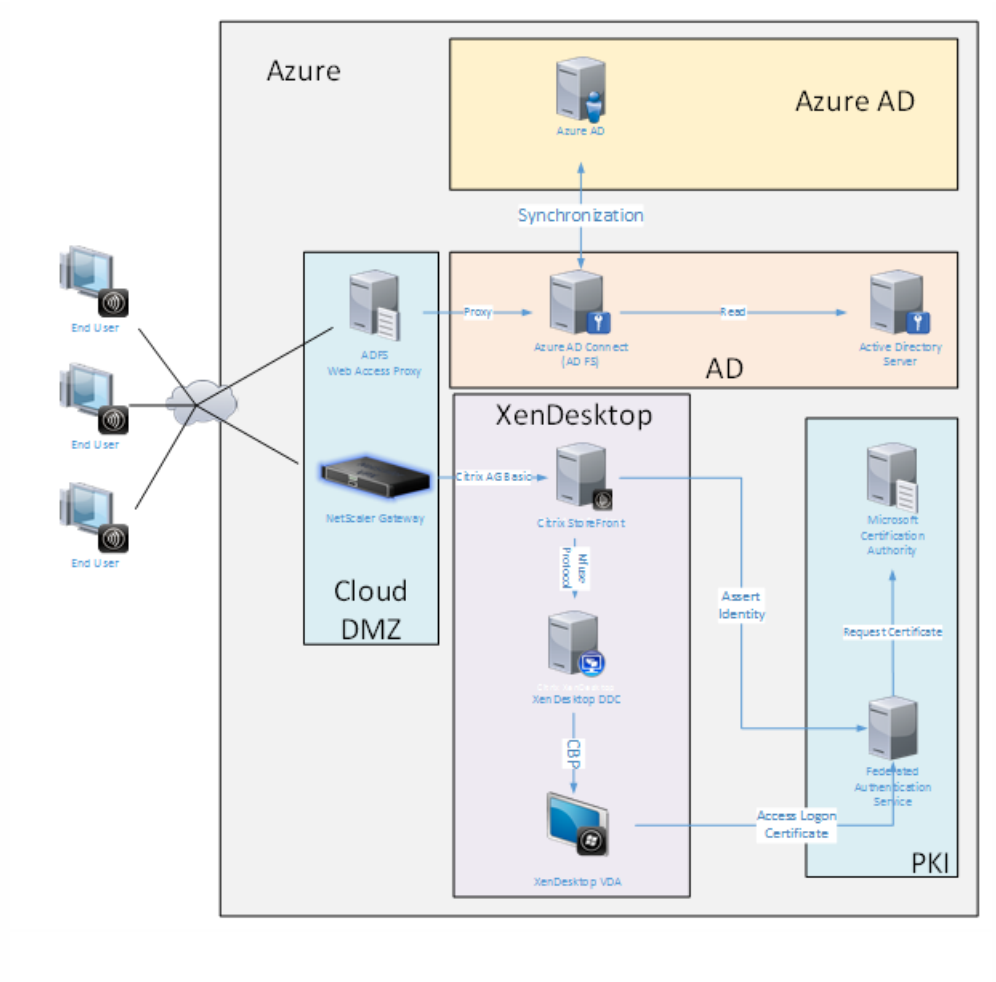



# Architektur

Diese Architektur repliziert innerhalb von Azure ein herkömmliches Unternehmensnetzwerk unter Integration moderner Cloudtechnologien, wie Azure Active Directory und Office 365. Die Endbenutzer werden alle als Remotebenutzer angesehen, das Konzept eines Büro-Intranets kommt nicht zur Anwendung.

Das Modell kann auch in Unternehmen mit lokalen Systemen verwendet werden, da die Azure AD Connect-Synchronisierung eine Verbindung mit Azure über das Internet herstellen kann.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Sichere Verbindungen und Single Sign-On, wie sie konventionell per LAN mit Firewall und Kerberos/NTLM-Authentifizierung realisiert wurden, werden in dieser Architektur durch TLS-Verbindungen mit Azure und SAML ersetzt. Neue Dienste werden als Azure-Anwendungen, die Mitglied von Azure AD sind, erstellt. Vorhandene Anwendungen, die Active Directory erfordern (z. B. eine SQL Server-Datenbank), können mit einer Standard-AD-Server-VM im IaaS-Teil des Azure-Clouddiensts ausgeführt werden.

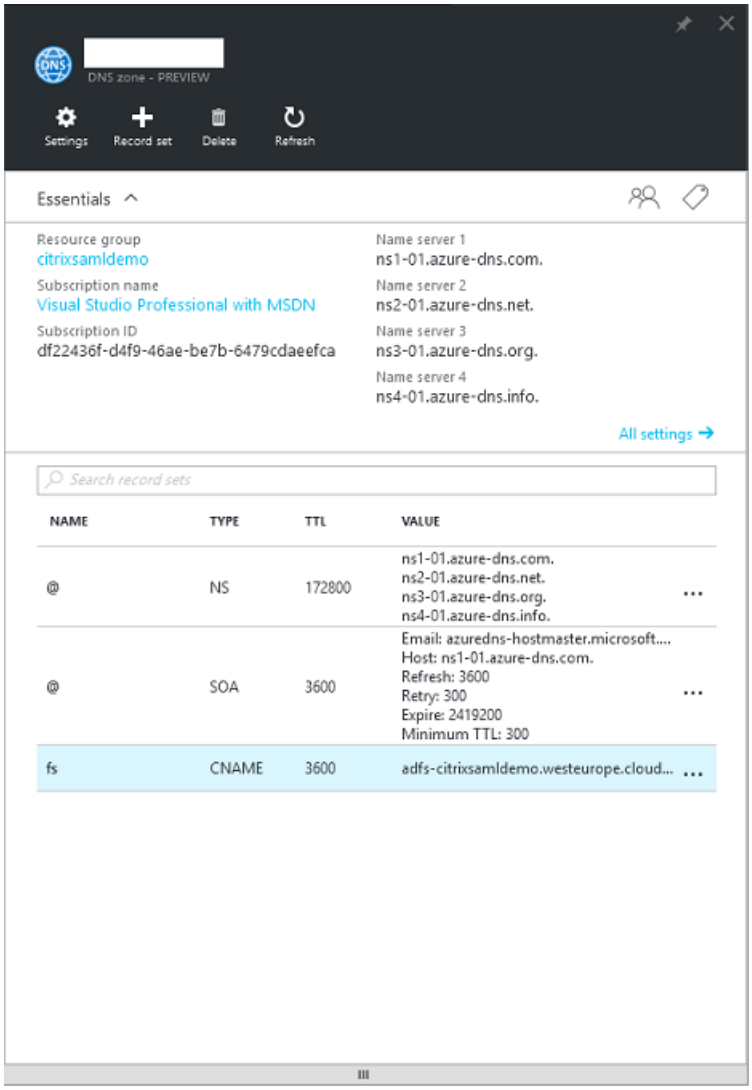
Wenn ein Benutzer eine herkömmliche Anwendung startet, erfolgt der Zugriff über die mit XenApp bzw. XenDesktop veröffentlichte Anwendung. Die verschiedenen Anwendungstypen werden auf der Seite **Azure-Anwendungen** unter Verwendung der Microsoft Edge-Single Sign-On-Features sortiert. Microsoft stellt außerdem Android- und iOS-Apps zur Verfügung, die Azure-Anwendungen aufzählen und starten können.

# Erstellen einer DNS-Zone

Für Azure AD muss der Administrator eine öffentliche DNS-Adresse registrieren und die Delegierungszone für das Domänennamensuffix steuern. Hierfür kann das Azure-Feature "DNS-Zone" verwendet werden.

Im vorliegenden Beispiel lautet der Name der DNS-Zone "citrixsamldemo.net".


© 1999-2017 Citrix Systems, Inc. All rights reserved.




In der Konsole werden die Namen der Azure-DNS-Namensserver angezeigt. Auf diese muss in den NS-Einträgen der DNS-Registrierungsstelle für die Zone verwiesen werden (z. B. citrixsamldemo.net. NS n1-01.azure-dns.com).

Beim Hinzufügen von Verweisen auf VMs, die in Azure ausgeführt werden, verwendet man am einfachsten den CNAME-Zeiger auf den in Azure verwalteten DNS-Eintrag für die jeweilige VM. Wenn sich die IP-Adresse der VM ändert, müssen Sie dann die DNS-Zonendatei nicht manuell aktualisieren.

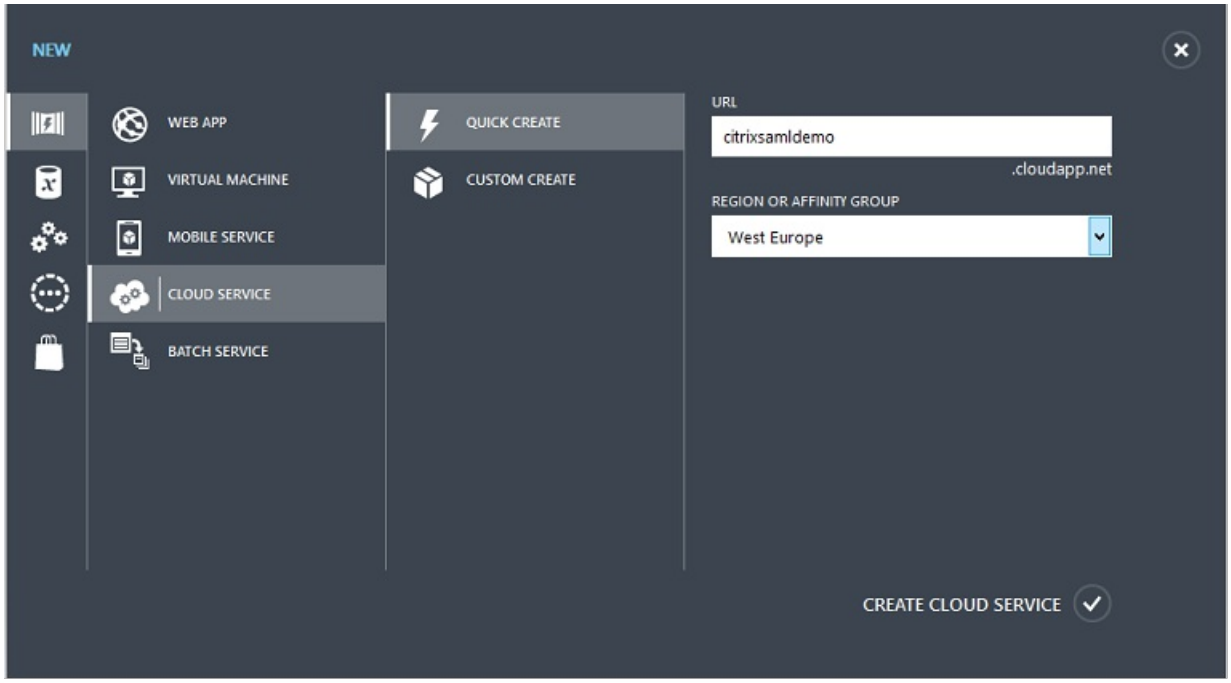
In dieser Bereitstellung stimmen internes und externes DNS-Adresssuffix überein. Die Domäne ist citrixsamldemo.net und verwendet Split DNS (10.0.0.* intern).

Fügen Sie den Eintrag "fs.citrixsamldemo.net" hinzu, der auf den Webanwendungsproxyserver verweist (mit Zeiger auf wap-citrixsamldemo... oben). Dies ist der Verbunddienst für diese Zone.

# Erstellen eines Clouddiensts

In diesem Beispiel wird eine Citrix Umgebung einschließlich einer AD-Umgebung mit einem in Azure ausgeführten AD FS-Server konfiguriert. Ein Clouddienst wird unter dem Namen "citrixsamldemo" erstellt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

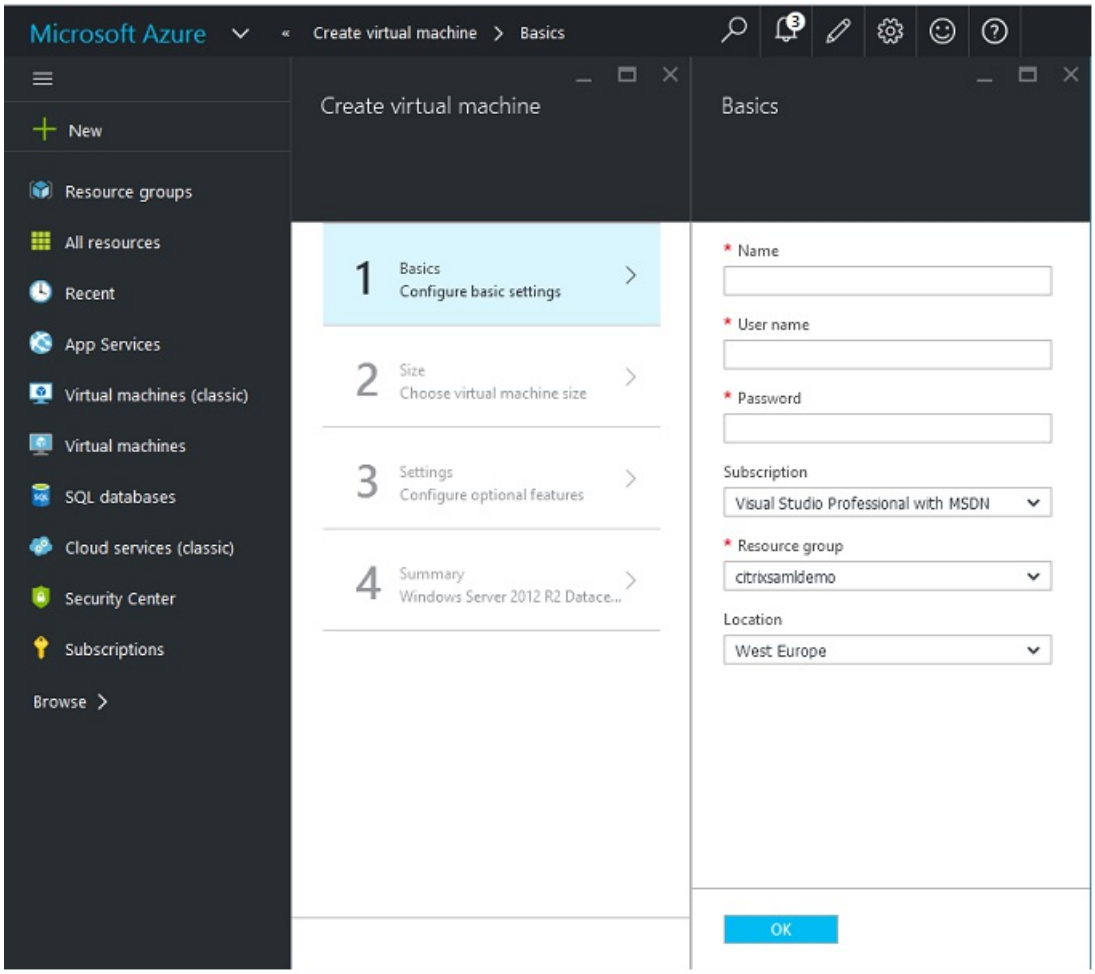



# Erstellen virtueller Windows-Maschinen

Erstellen Sie fünf Windows-VMs, die im Clouddienst ausgeführt werden:

- Domänencontroller (domaincontrol)
- Azure Connect AD FS-Server (adfs)
- AD FS-Proxy für den Webzugriff (Webanwendungsproxy, kein Mitglied einer Domäne)
- Citrix XenDesktop Delivery Controller (ddc)
- Citrix XenDesktop Virtual Delivery Agent (vda)


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Domänencontroller**

- Fügen Sie die Rollen **DNS-Server** und **Active Directory-Domänendienste** hinzu, um eine Active Directory-Standardbereitstellung zu erstellen (in diesem Beispiel citrixsamldemo. net). Nach Abschluss der Domänenpromotion fügen Sie die Rolle **Active Directory-Zertifikatdienste** hinzu.
- Erstellen Sie ein normales Benutzerkonto für Tests (z. B. George@citrixsamldemo.net).
- Da auf diesem Server DNS intern ausgeführt wird, müssen alle Server zur DNS-Auflösung auf diesem Server verweisen. Die entsprechende Einstellung können Sie über die Seite mit den Azure-DNS-Einstellungen vornehmen. (Weitere Informationen finden Sie im Anhang).

**AD FS-Controller und Webanwendungsproxyserver**

- Fügen Sie den AD FS-Server der Domäne citrixsamldemo hinzu. Der Webanwendungsproxyserver muss in einer isolierten Arbeitsgruppe bleiben. Registrieren Sie daher manuell eine DNS-Adresse beim AD-DNS.
- Führen Sie an diesen Servern das Cmdlet **Enable-PSRemoting –Force** aus, um PS-Remoting aus dem Azure AD Connect-Tool über Firewalls zuzulassen.

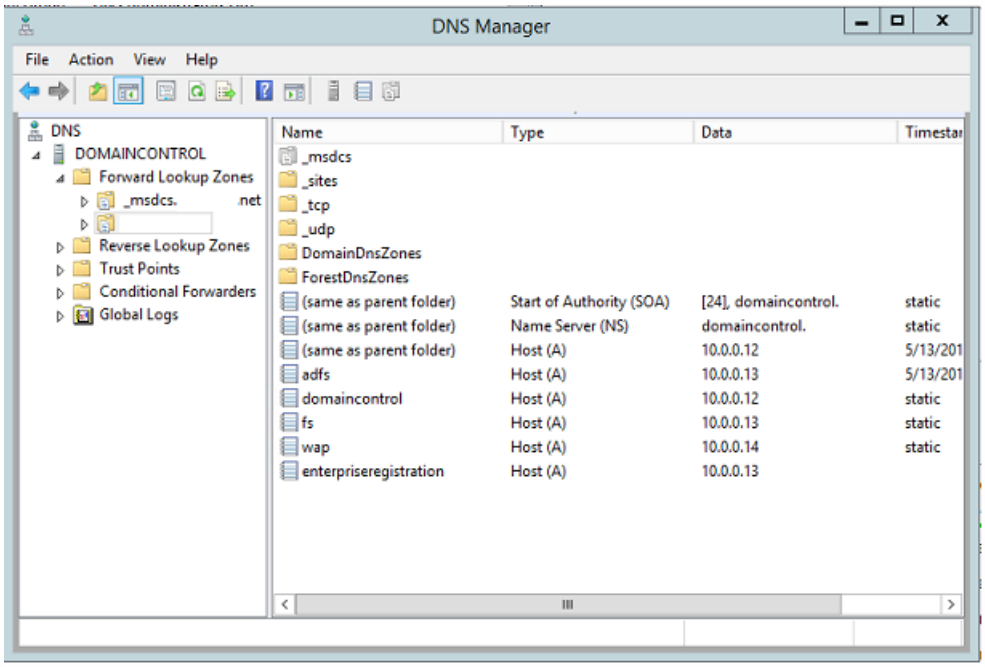
**XenDesktop Delivery Controller und VDA**

- Installieren Sie den XenApp- bzw. XenDesktop Delivery Controller und VDA auf den verbleibenden beiden Windows-Servern, die zur Domäne citrixsamldemo gehören.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren eines internen DNS

Nach Installation des Domänencontrollers konfigurieren Sie den DNS-Server für die interne citrixsamldemo.net-Dimension und als Weiterleiter an einen externen DNS-Server (z. B.: 8.8.8.8).

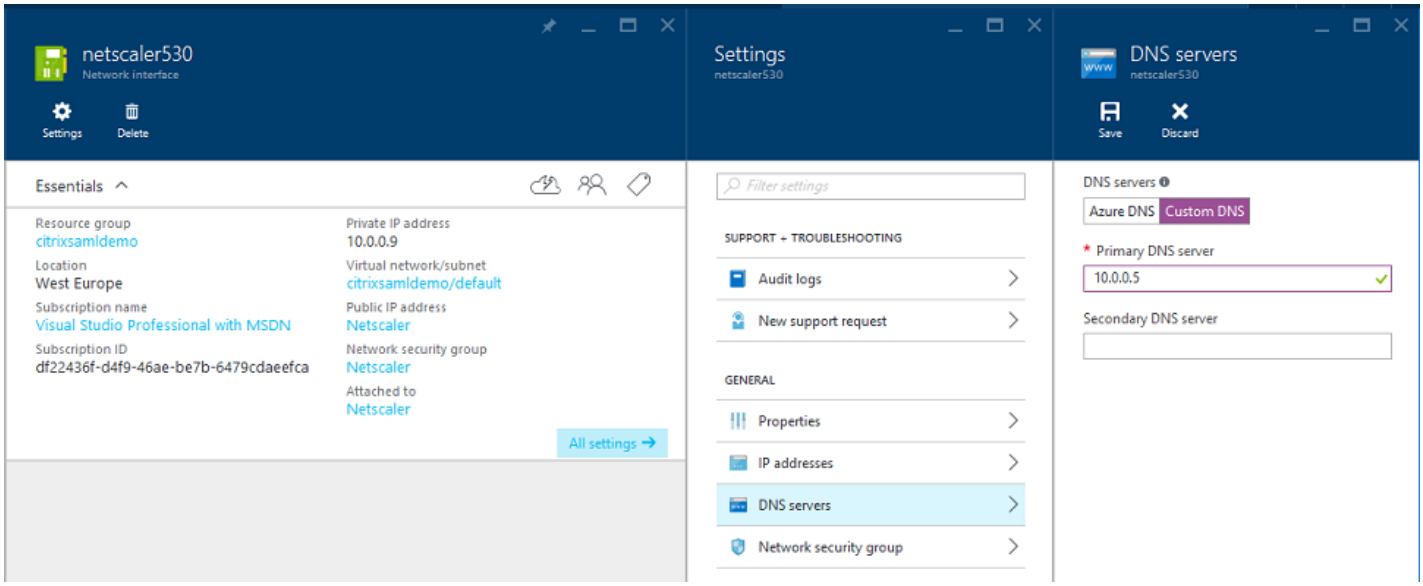



Fügen Sie für folgende Elemente einen statischen Eintrag hinzu:

- wap.citrixsamldemo.net (die Webanwendungsproxy-VM wird nicht der Domäne hinzugefügt)
- fs.citrixsamldemo.net (Adresse des internen Verbundservers)
- enterpriseregistration.citrixsaml.net (identisch mit fs.citrixsamldemo.net)

Alle in Azure ausgeführten VMs müssen zur ausschließlichen Verwendung dieses DNS-Servers konfiguriert werden. Sie können diese Konfiguration über die Netzwerkschnittstellen-GUI durchführen.

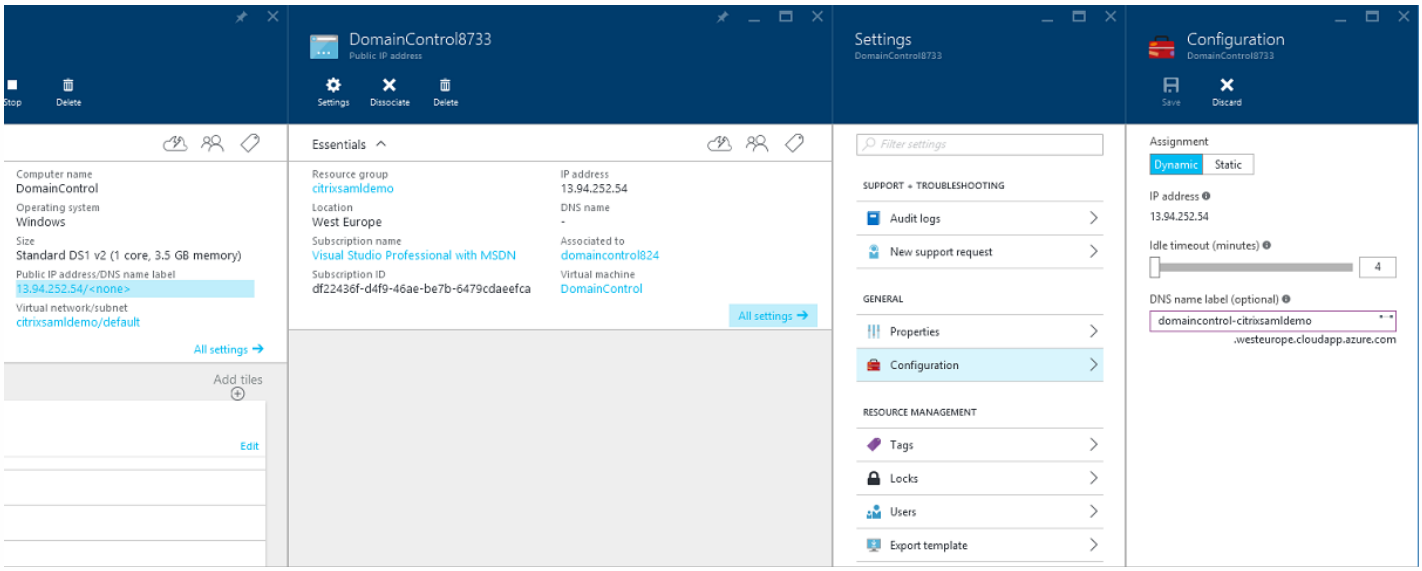

© 1999-2017 Citrix Systems, Inc. All rights reserved.




Standardmäßig wird die interne IP-Adresse (10.0.0.9) dynamisch zugewiesen. Sie können die IP-Adresse über die zugehörige Einstellung bleibend zuweisen. Diesen Schritt müssen Sie für den Webanwendungsproxyserver und den Domänencontroller durchführen.

# Konfigurieren einer externen DNS-Adresse

Wenn eine virtuelle Maschine ausgeführt wird, verwendet Azure seinen eigenen DNS-Zonenserver, der auf die aktuelle, der VM zugewiesene, öffentliche IP-Adresse verweist. Dies kann als nützliches Feature aktiviert werden, da Azure standardmäßig IP-Adressen bei jedem VM-Start zuweist.




In diesem Beispiel wird dem Domänencontroller die DNS-Adresse "domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com" zugewiesen.

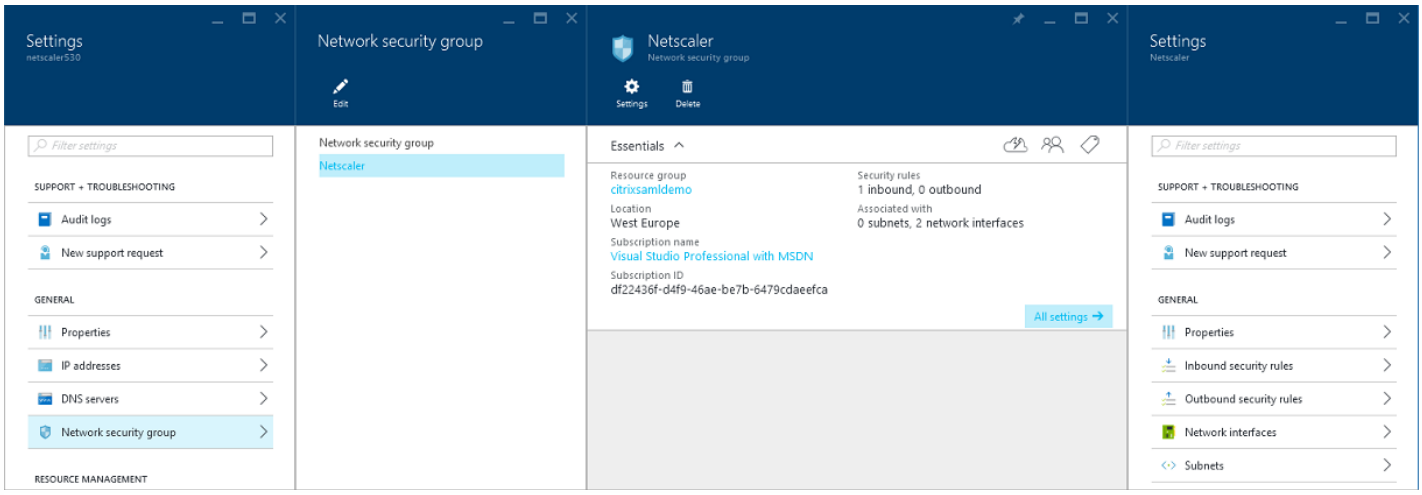
Nach Abschluss der Remotekonfiguration dürfen öffentliche IP-Adressen nur für die Webanwendungsproxy- und die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler-VMs aktiviert sein. (Während der Konfiguration wird die öffentliche IP-Adresse für den RDP-Zugriff auf die Umgebung verwendet).

# Konfigurieren von Sicherheitsgruppen

Von der Azure-Cloud werden Firewall-Regeln für den TCP/UDP-Zugriff auf VMs aus dem Internet mithilfe von Sicherheitsgruppen verwaltet. Standardmäßig lassen alle VMs RDP-Zugriff zu. Der NetScaler-Server und der Webanwendungsproxyserver müssen außerdem TLS an Port 443 zulassen.



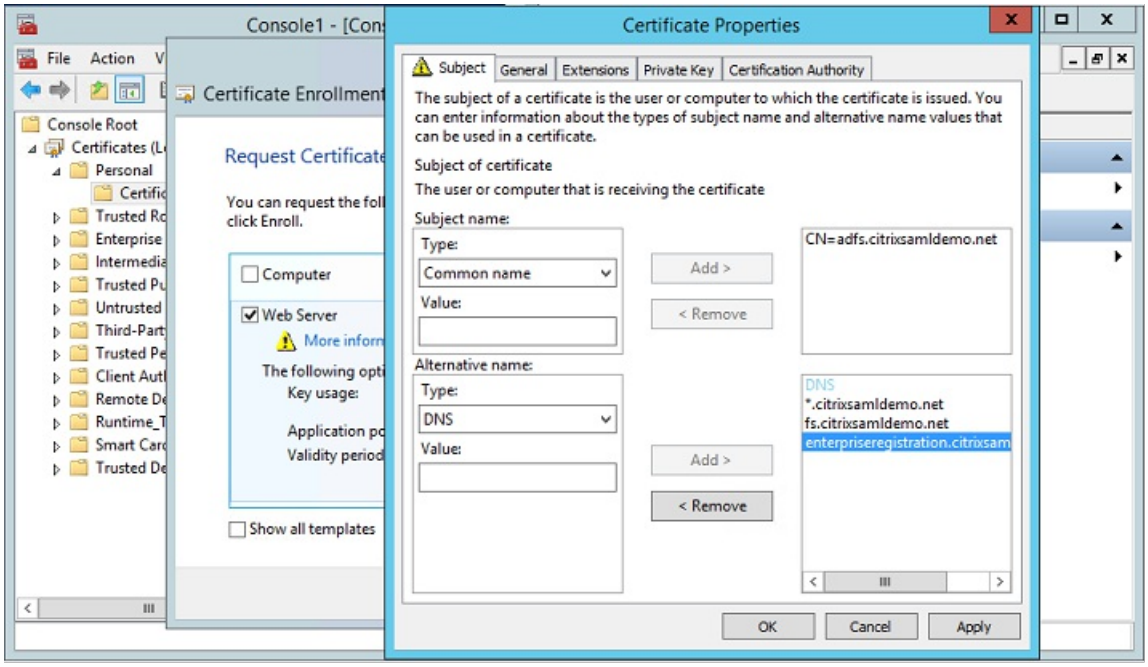

# Erstellen eines AD FS-Zertifikats

Aktivieren Sie die Zertifikatvorlage **Webserver** in der Microsoft-Zertifizierungsstelle (CA). Dies ermöglicht die Erstellung eines Zertifikats mit benutzerdefinierten DNS-Adressen, das einschließlich privatem Schlüssel in eine PFX-Datei exportiert werden kann. Sie müssen dieses Zertifikat auf dem AD FS-Server und dem Webanwendungsproxyserver installieren, damit die PFX-Datei bevorzugte Option ist.

Stellen Sie ein Webserverzertifikat mit folgenden Antragstellernamen aus:

- Commonname:
  - adfs.citrixsamldemo.net (Computername)
- SubjectAltname:
  - *.citrixsamldemo.net (Zonenname)
  - fs.citrixsamldemo. net (Eintrag in DNS)
  - enterpriseregistration.citrixsamldemo.net


© 1999-2017 Citrix Systems, Inc. All rights reserved.



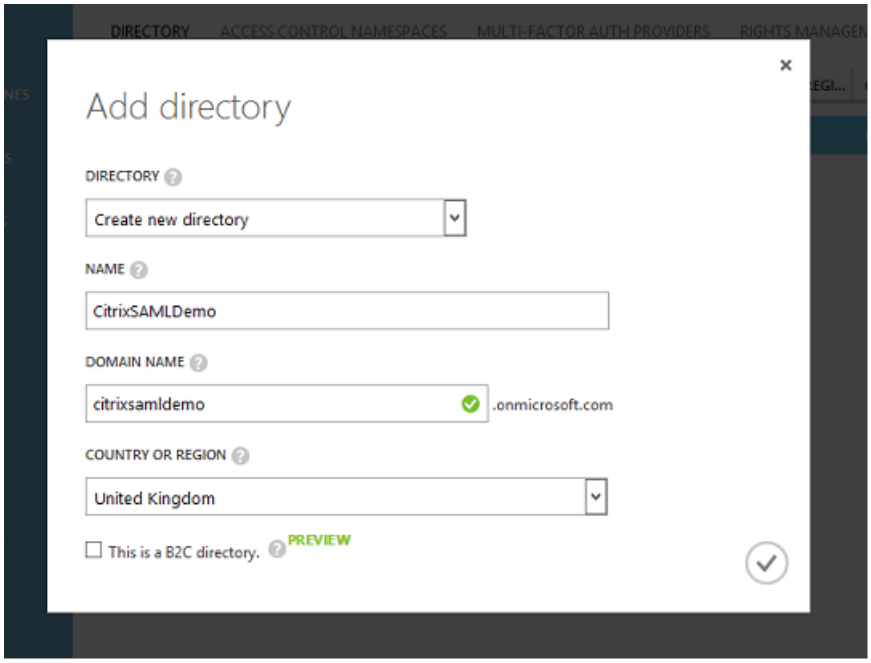

Exportieren Sie das Zertifikat mitsamt einem kennwortgeschützten privaten Schlüssel in eine PFX-Datei.

# Einrichten von Azure Active Directory

In diesem Abschnitt wird erläutert, wie eine neue Instanz von Azure AD eingerichtet und Benutzeridentitäten für die Windows 10-Einbindung in Azure AD erstellt werden.

**Erstellen eines Verzeichnisses**

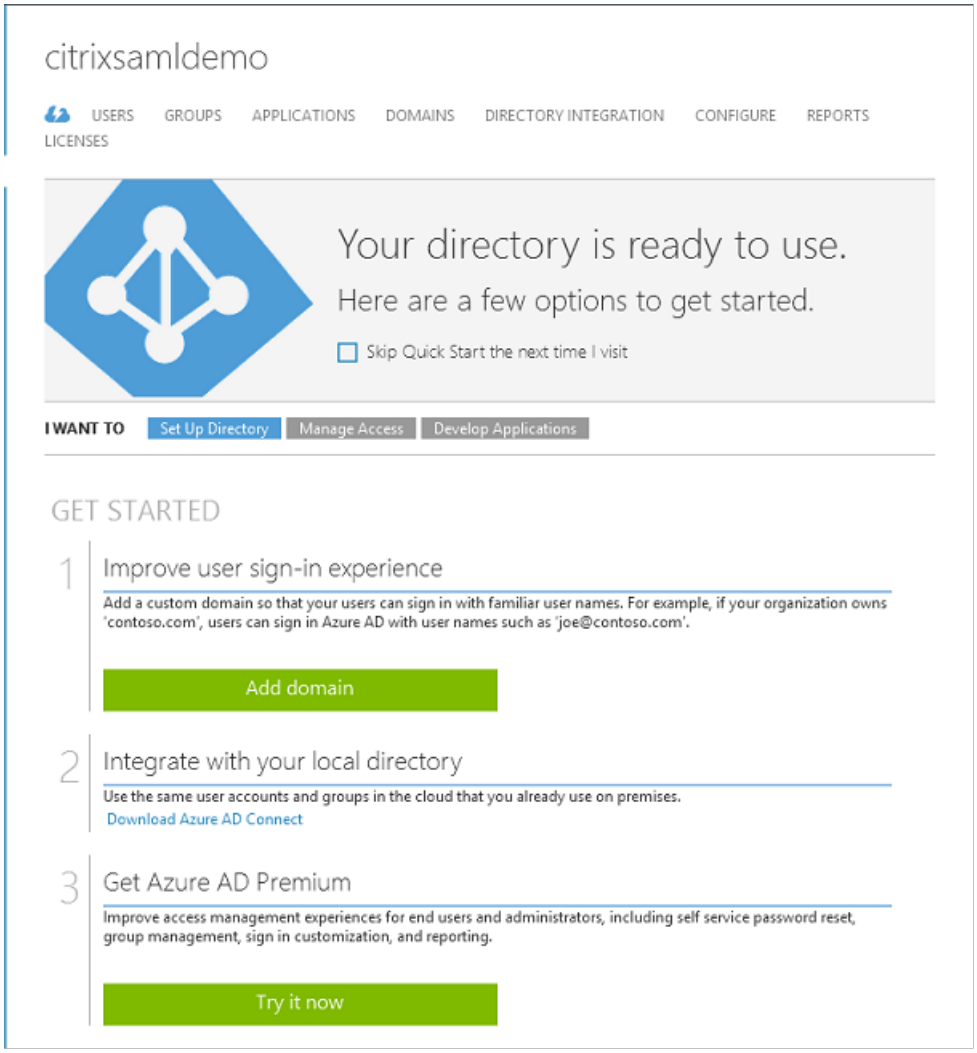
Melden Sie sich beim Azure-Portal an und erstellen Sie ein Verzeichnis.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

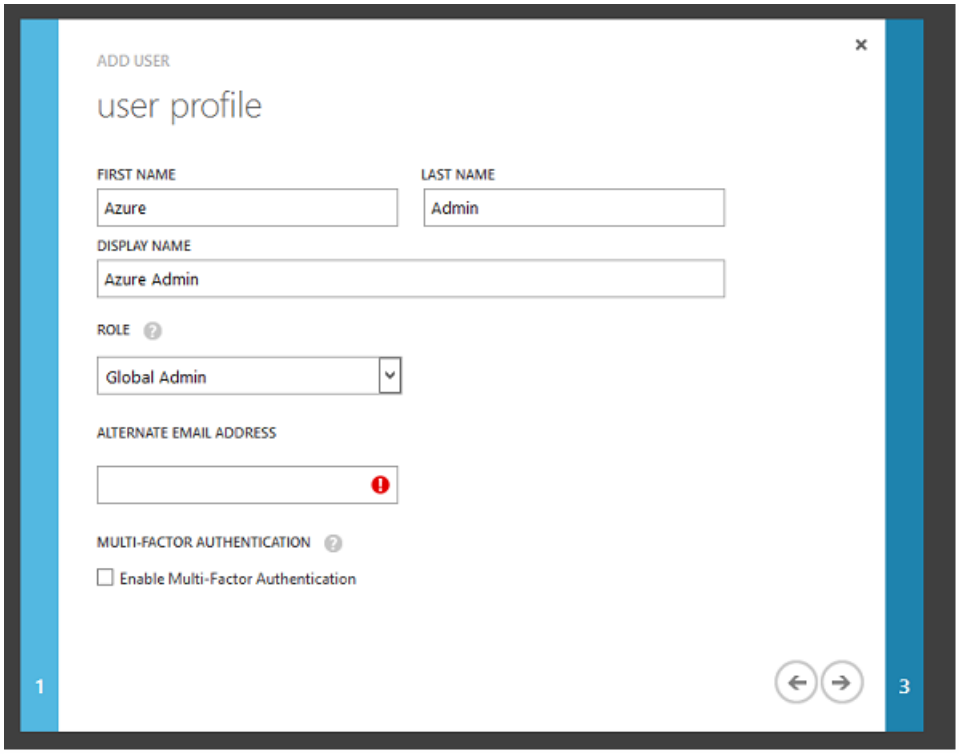
Zum Abschluss wird die Seite "Zusammenfassung" angezeigt.




**Erstellen eines globalen Administrators (AzureAdmin)**

Erstellen Sie einen globalen Administrator in Azure (in diesem Beispiel AzureAdmin@citrixsamldemo.onmicrosoft.com) und melden Sie sich mit dem neuen Konto an, um ein Kennwort einzurichten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Registrieren der Domäne bei Azure AD**

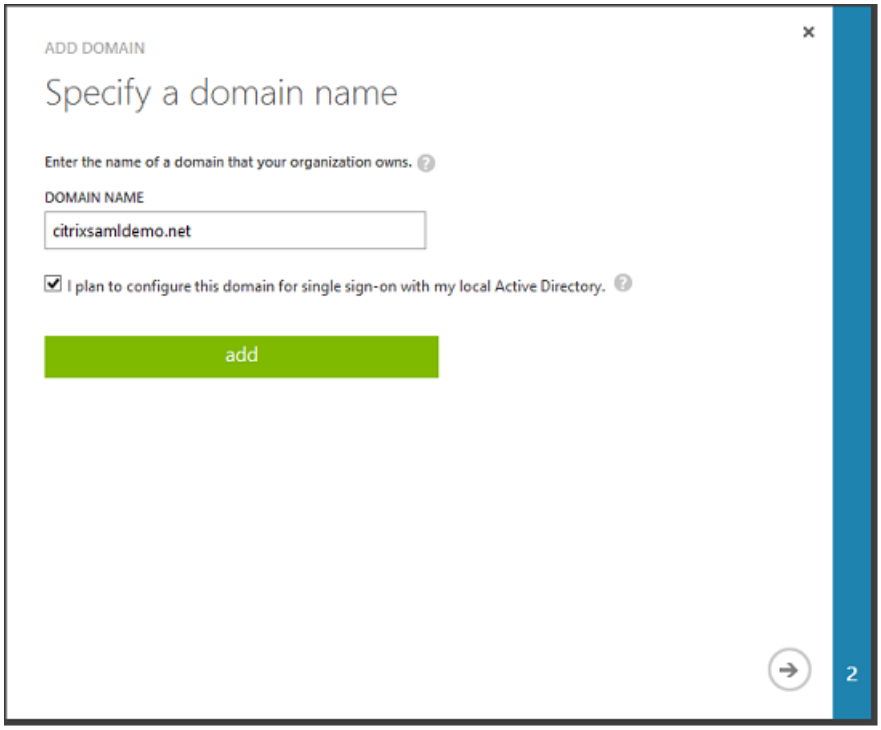
Standardmäßig werden Benutzer anhand einer E-Mail-Adresse im Format <*benutzer.name*>@<*firma*>.*onmicrosoft.com* identifiziert.

Dies funktioniert zwar ohne weitere Konfiguration, eine E-Mail-Adresse im Standardformat ist jedoch besser; sie sollte möglichst dem E-Mail-Konto des Endbenutzers entsprechen: @.com.

Die Aktion **Domäne hinzufügen** dient zum Konfigurieren der Umleitung von der tatsächlichen Unternehmensdomäne. In diesem Beispiel wird citrixsamldemo.net verwendet.

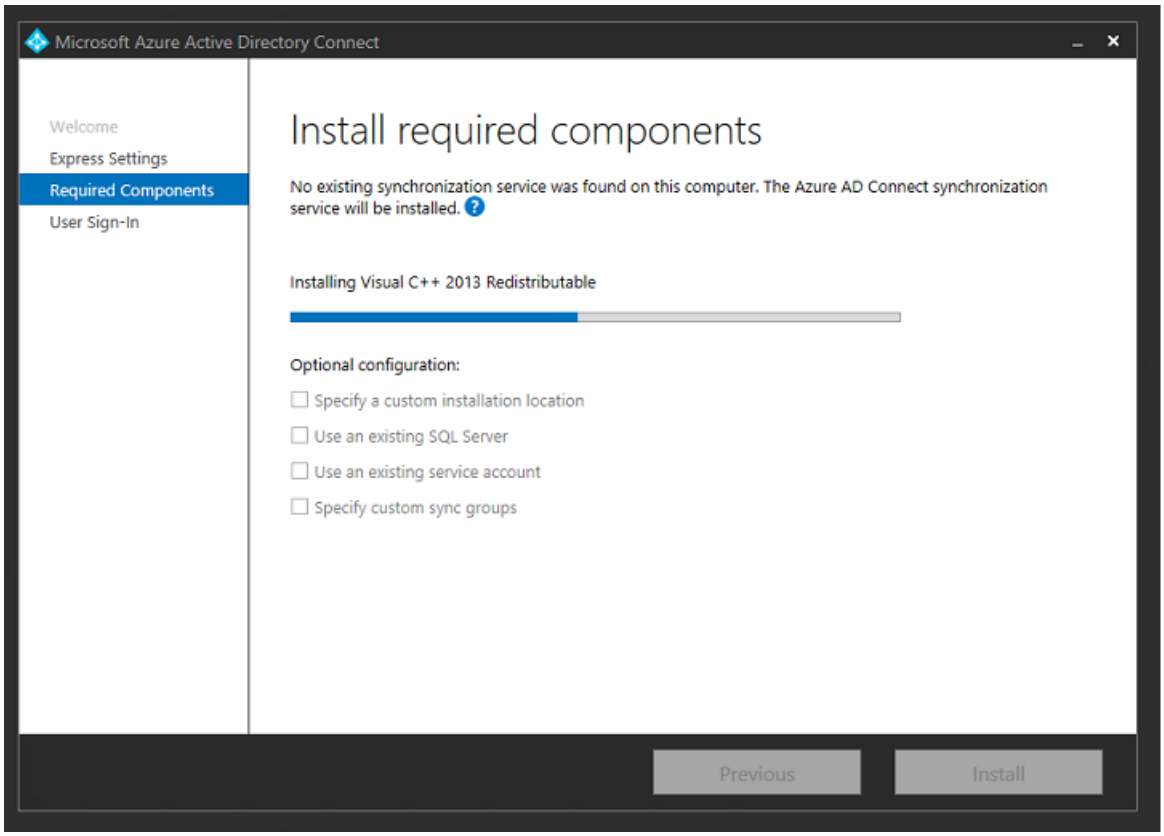
Wenn Sie AD FS für Single Sign-On einrichten, aktivieren Sie das Kontrollkästchen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Installieren von Azure AD Connect**

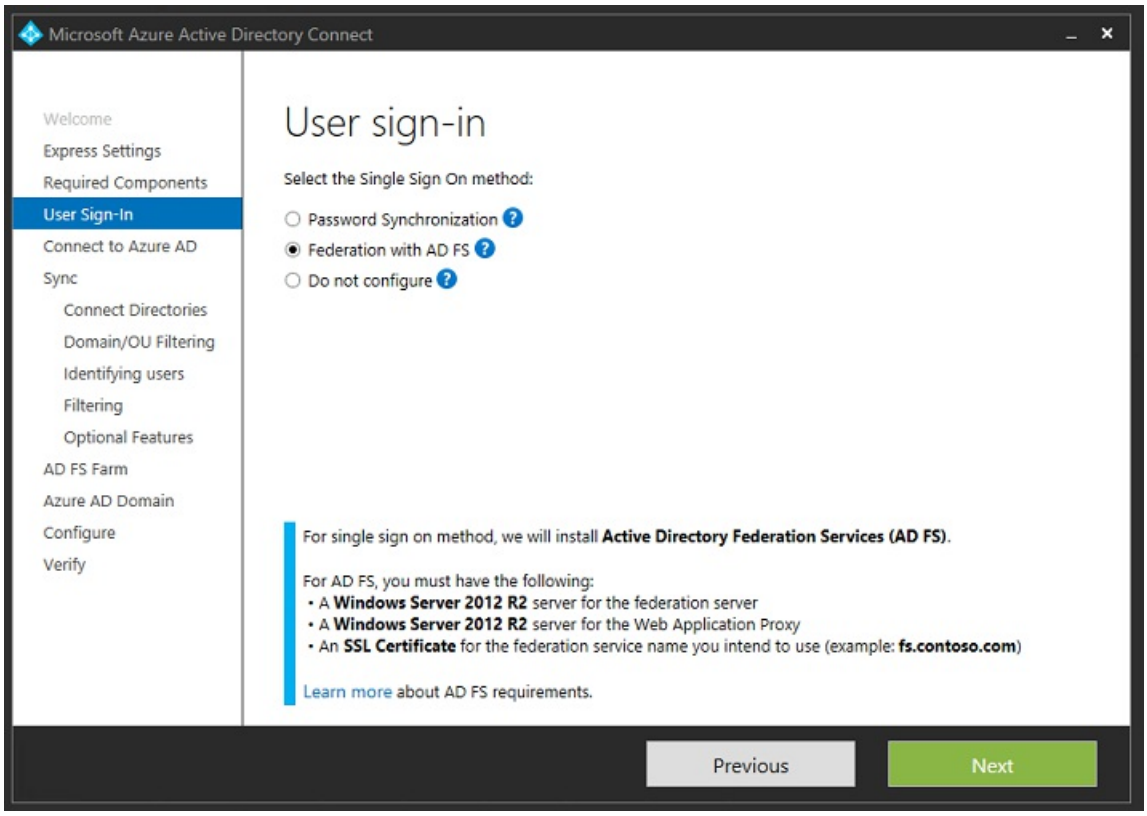
In Schritt 2 der Azure AD-Konfiguration werden Sie auf die Downloadseite für Azure AD Connect umgeleitet. Installieren Sie dieses Tool auf der AD FS-VM. Verwenden Sie **Benutzerdefinierte Installation** anstelle von **Express-Einstellungen**, damit AD FS-Optionen verfügbar sind.



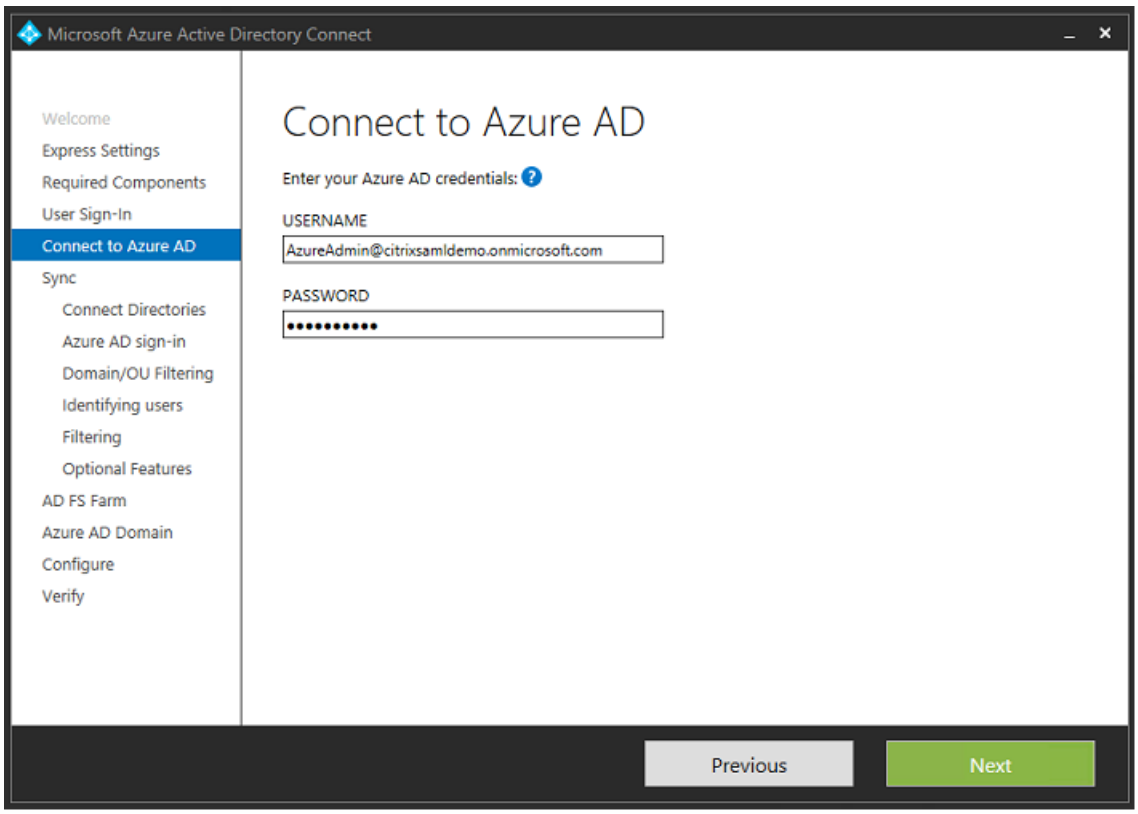


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wählen Sie die Single Sign-On-Option **Verbund mit AD FS**.



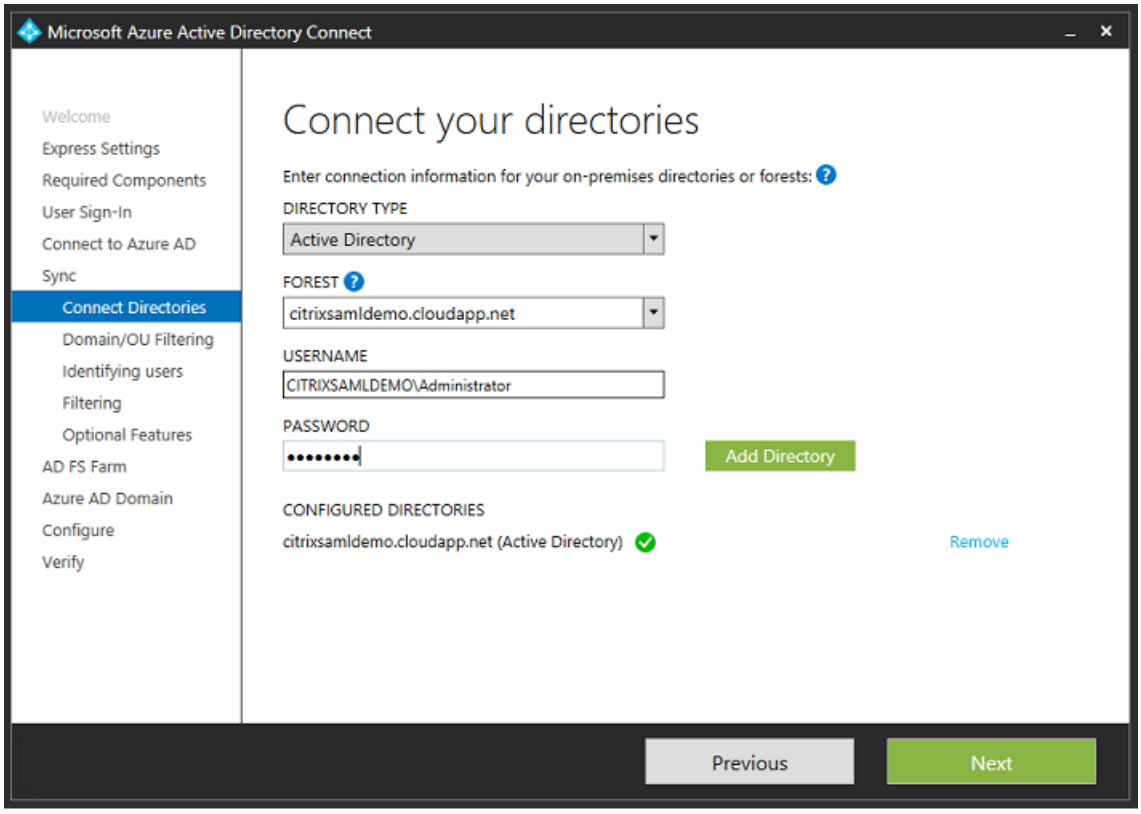

Stellen Sie eine Verbindung mit Azure unter Verwendung des zuvor erstellten Administratorkontos her.





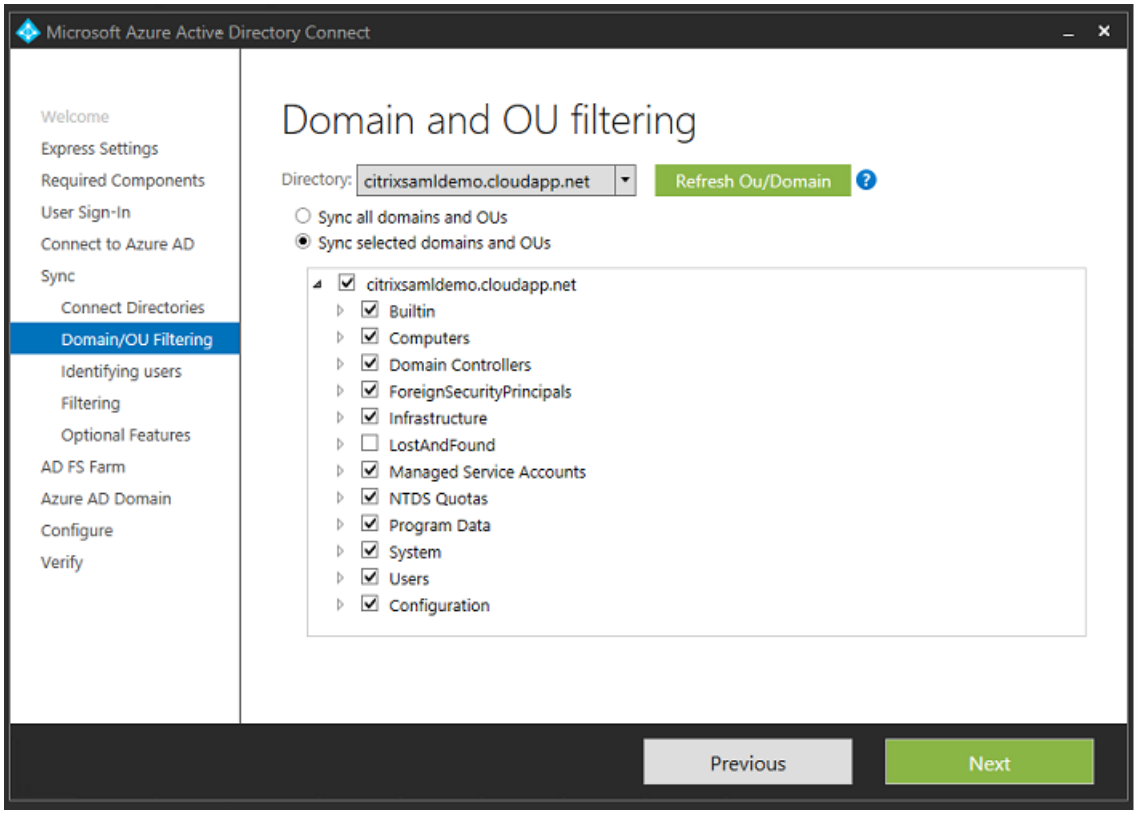
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wählen Sie die interne AD-Gesamtstruktur.

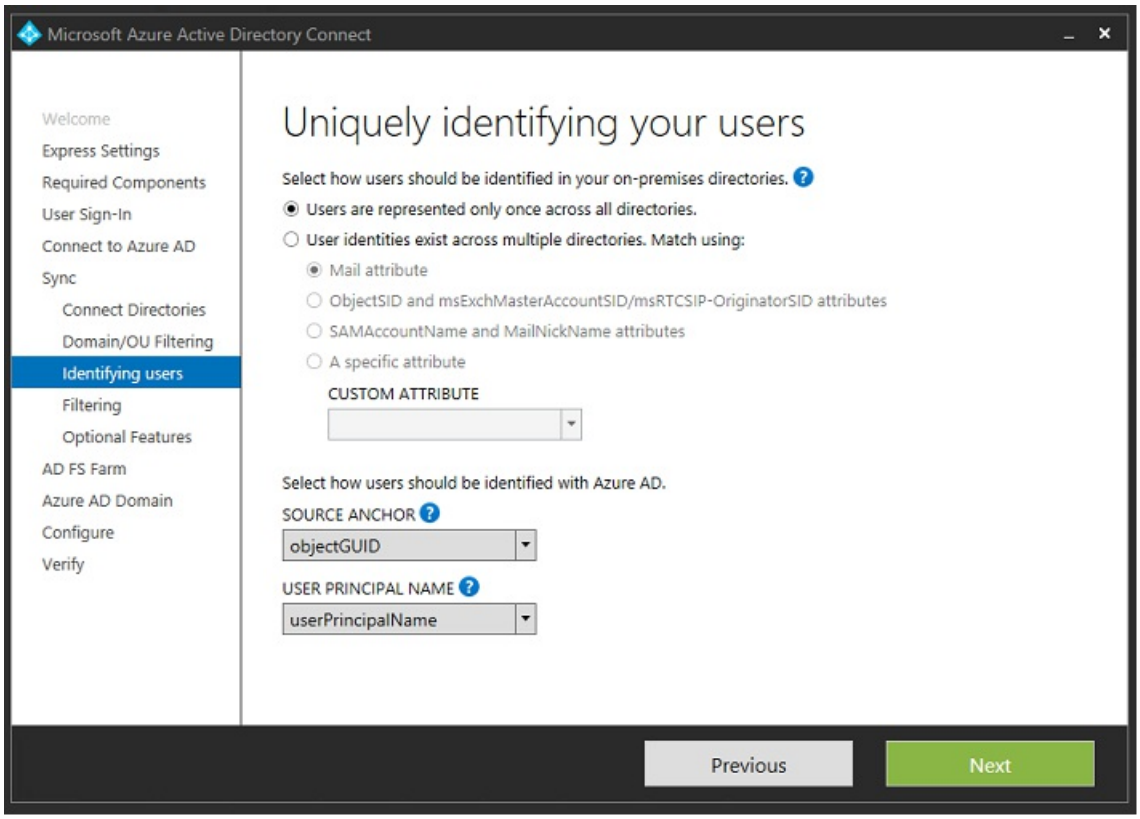



Synchronisieren Sie alle alten Active Directory-Objekte mit Azure AD.


© 1999-2017 Citrix Systems, Inc. All rights reserved.



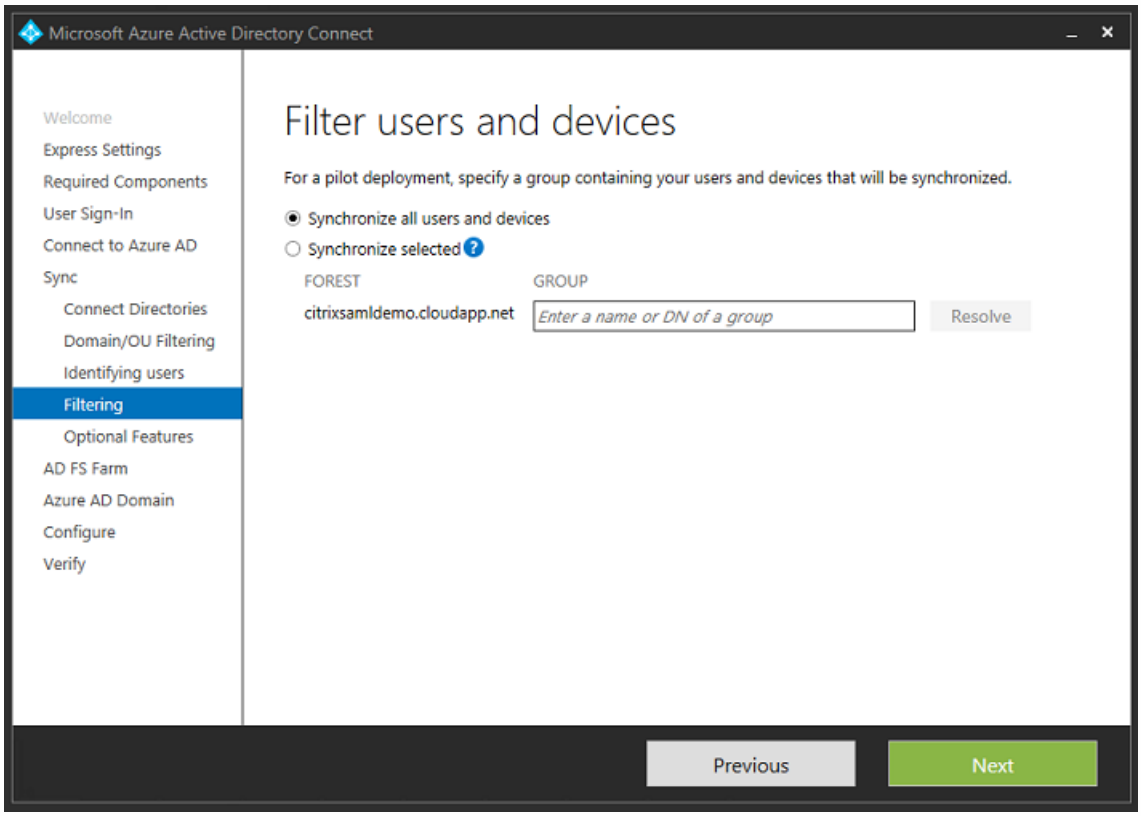

Bei einer einfachen Verzeichnisstruktur sind die Benutzernamen ausreichend eindeutig zur Identifizierung von Benutzern, die sich anmelden.



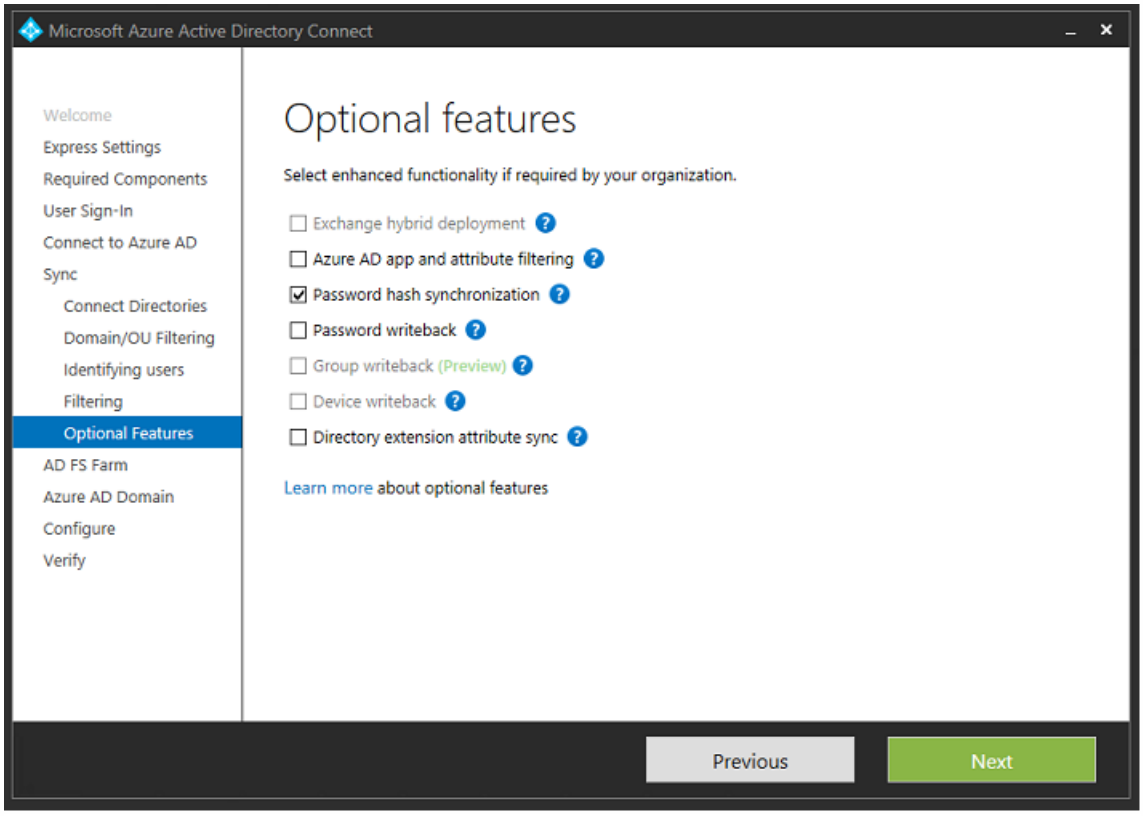


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Akzeptieren Sie die Standardfilteroptionen oder schränken Sie Benutzer und Geräte auf bestimmte Gruppen ein.



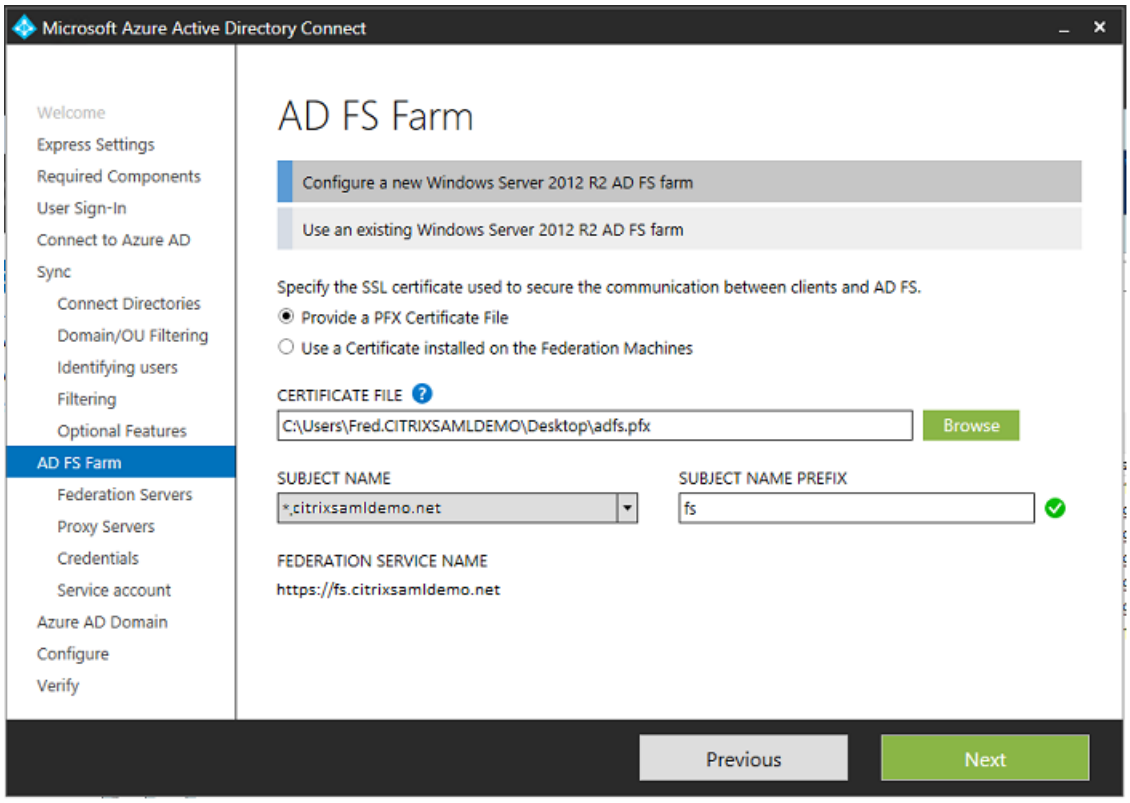

Falls gewünscht können Sie die Azure AD-Kennwörter mit Active Directory synchronisieren. Das ist für die AD FS-basierte Authentifizierung normalerweise nicht nötig.





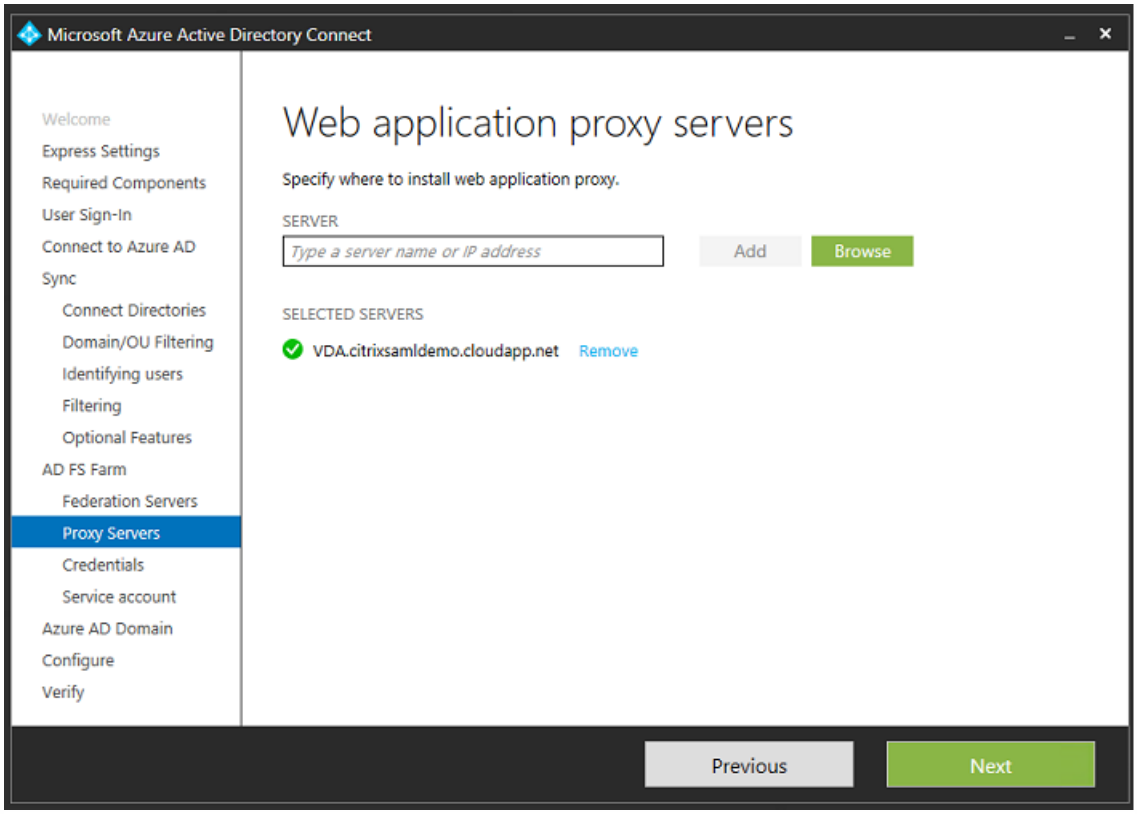
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wählen Sie die Zertifikat-PFX-Datei für AD FS unter Angabe von "fs.citrixsamldemo.net" als DNS-Namen aus.




Wenn Sie zur Auswahl eines Proxyservers aufgefordert werden, geben Sie die Adresse des wap.citrixsamldemo.net-Servers ein. Sie müssen u. U. das Cmdlet **Enable-PSRemoting –Force** als Administrator auf dem Webanwendungsproxyserver ausführen, damit Azure AD diesen konfigurieren kann.

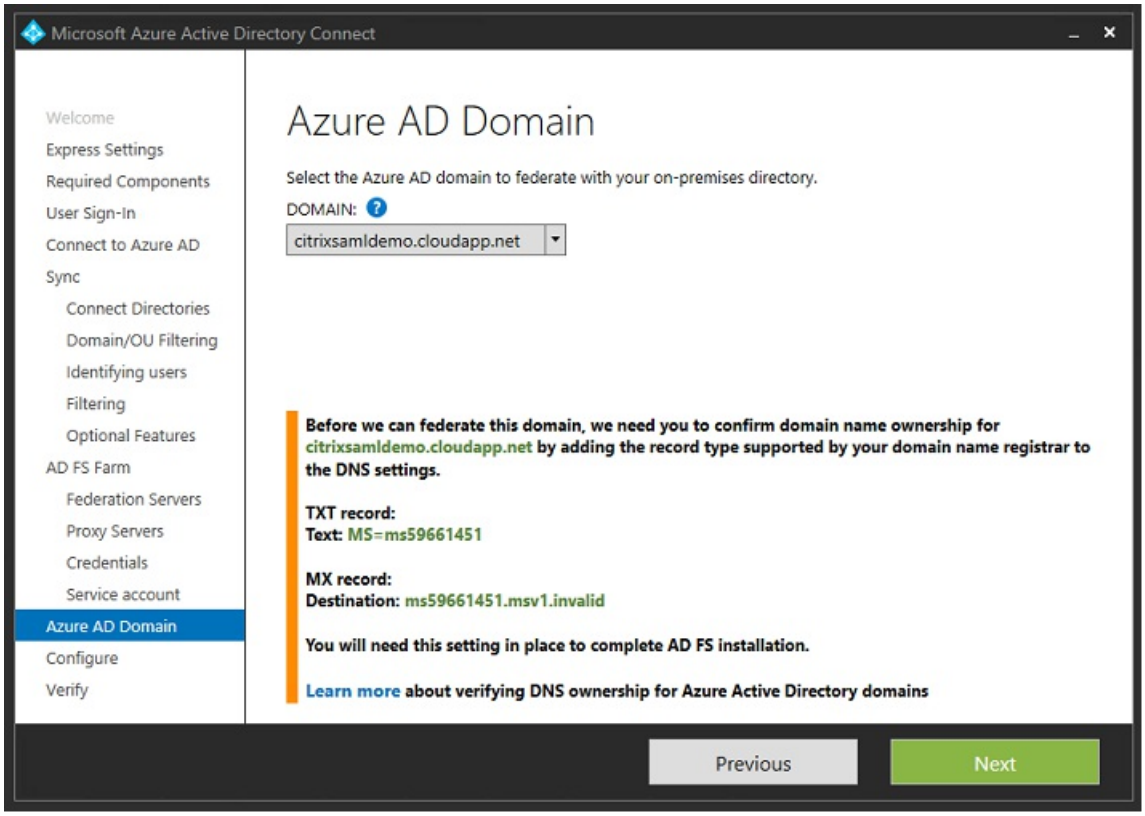

© 1999-2017 Citrix Systems, Inc. All rights reserved.



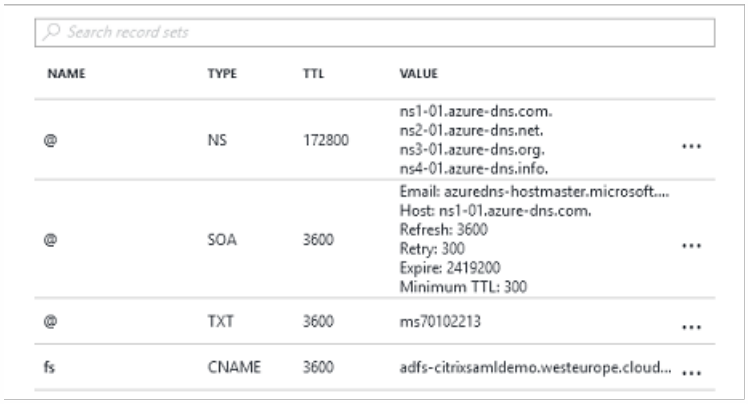

**Hinweis:** Wenn dieser Schritt aufgrund von Problemen mit der Remote PowerShell-Vertrauensstellung fehlschlägt, versuchen Sie den Beitritt des Webanwendungsproxyservers zur Domäne.

Verwenden Sie für die restlichen Schritte des Assistenten die Standardadministratorkennwörter und erstellen Sie ein Dienstkonto für AD FS. Von Azure AD Connect wird dann zur Überprüfung der Eigentümerschaft der DNS-Zone aufgefordert.

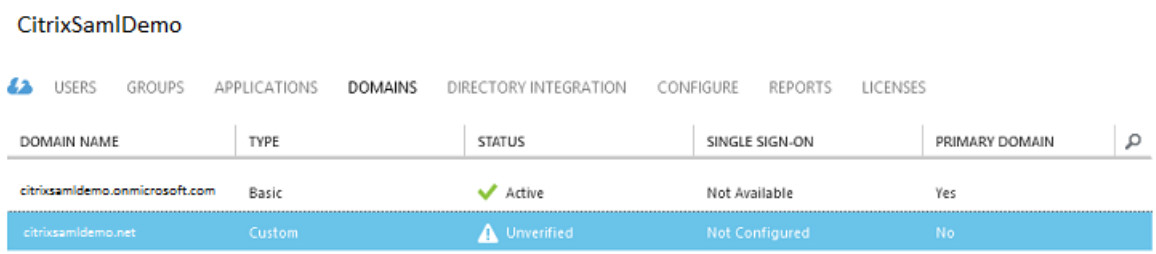

© 1999-2017 Citrix Systems, Inc. All rights reserved.




Fügen Sie die TXT- und MX-Einträge den DNS-Adresseinträgen in Azure hinzu.




Klicken Sie in der Azure-Verwaltungskonsole auf **Überprüfen**.

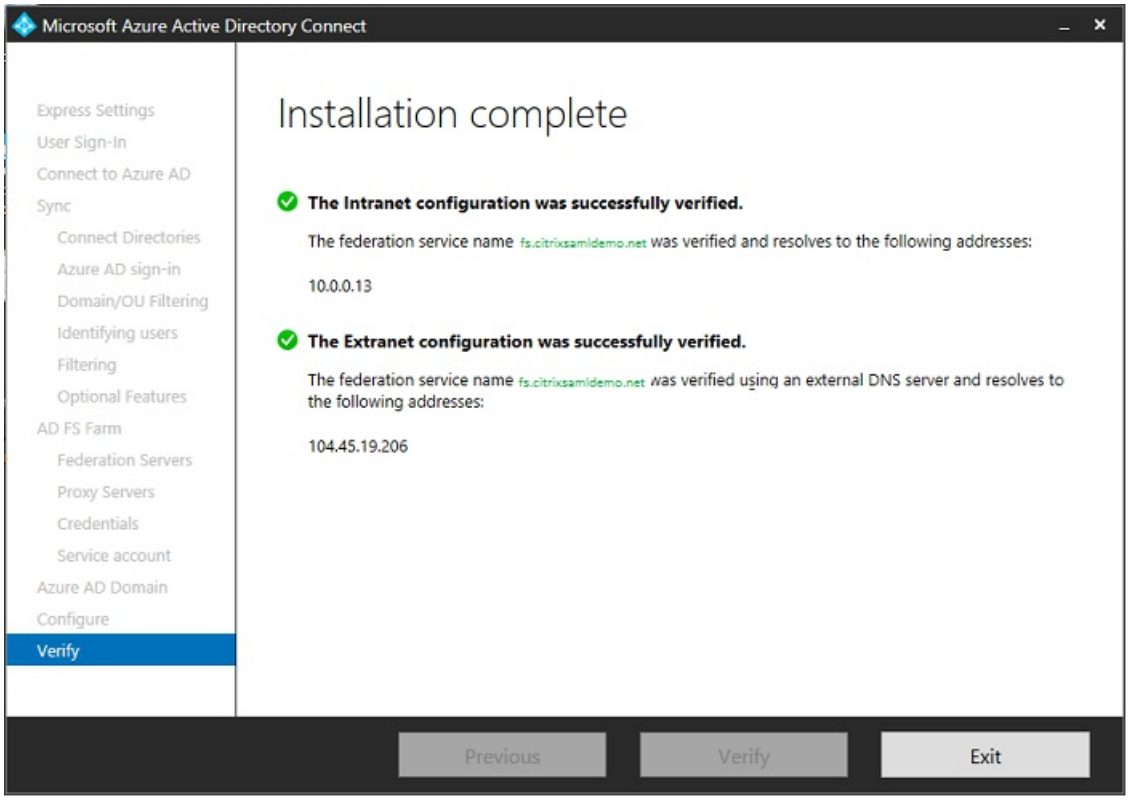




© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Hinweis:** Wenn dieser Schritt fehlschlägt, können Sie die Domäne vor Ausführung von Azure AD Connect überprüfen.

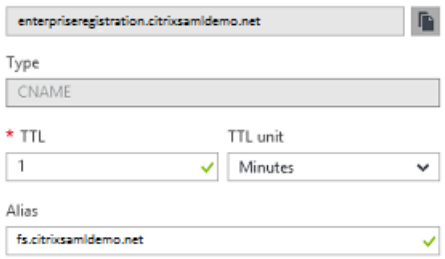
Nach Anschluss wird die externe Adresse fs.citrixsamldemo.net über Port 443 angesprochen.




# Aktivieren der Azure AD-Einbindung

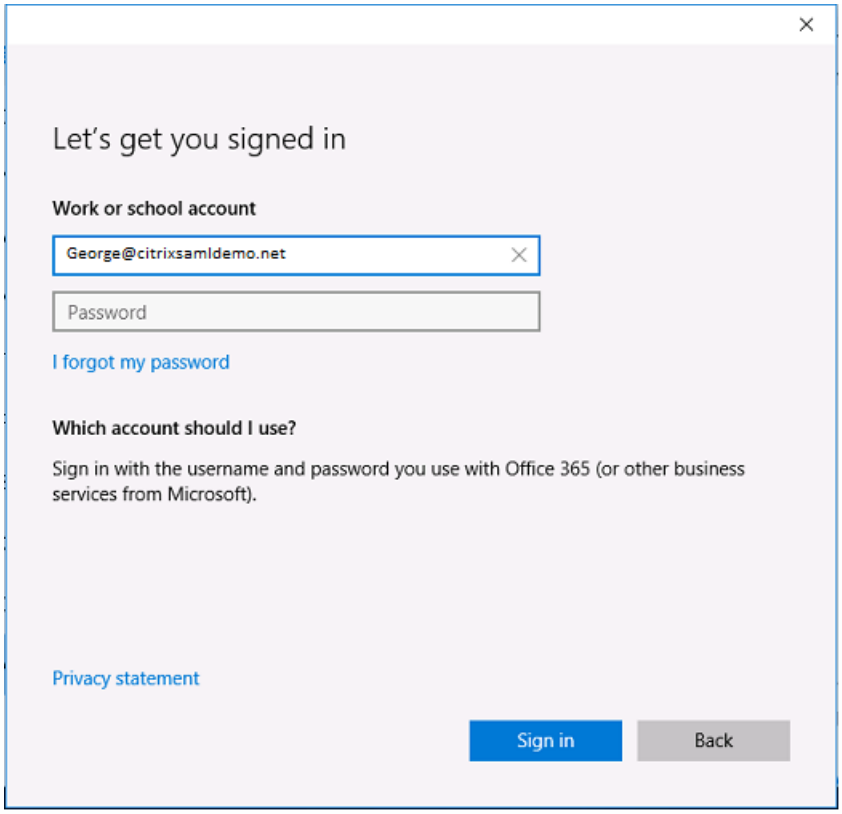
Wenn ein Benutzer eine E-Mail-Adresse eingibt, damit Windows 10 eine Einbindung in Azure AD durchführen kann, wird anhand des DNS-Suffixes ein CNAME DNS-Eintrag erstellt, der auf AD FS verweisen muss: enterpriseregistration..

In diesem Beispiel ist dies fs.citrixsamldemo.net.

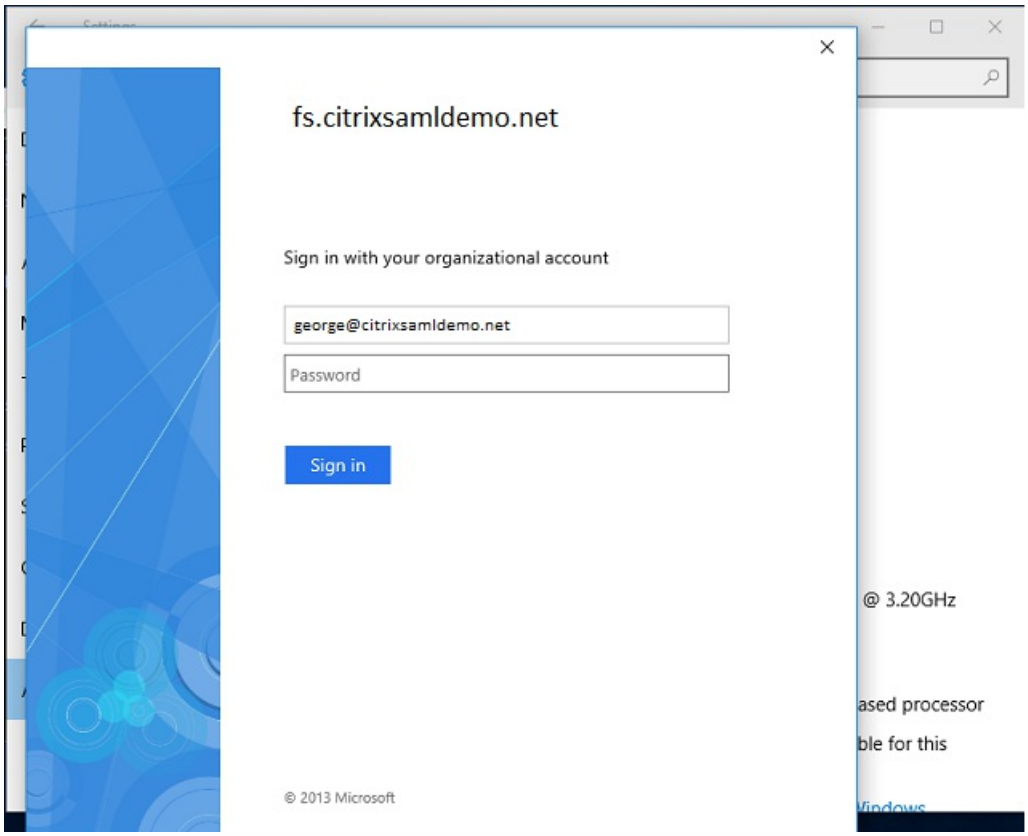



Wenn Sie keine öffentliche Zertifizierungsstelle verwenden, installieren Sie das AD FS-Stammzertifikat auf dem Windows 10-Computer, damit Windows dem AD FS-Server vertraut. Führen Sie einen Azure AD-Domänenbeitritt unter Verwendung des zuvor erstellten Standardbenutzerkontos durch.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

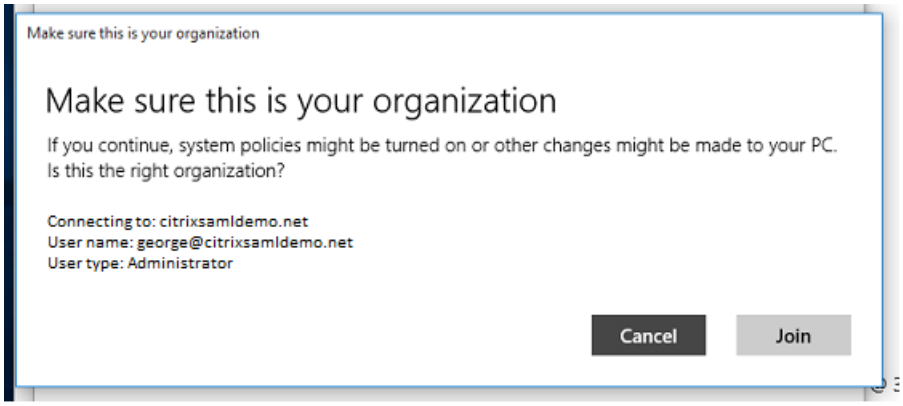


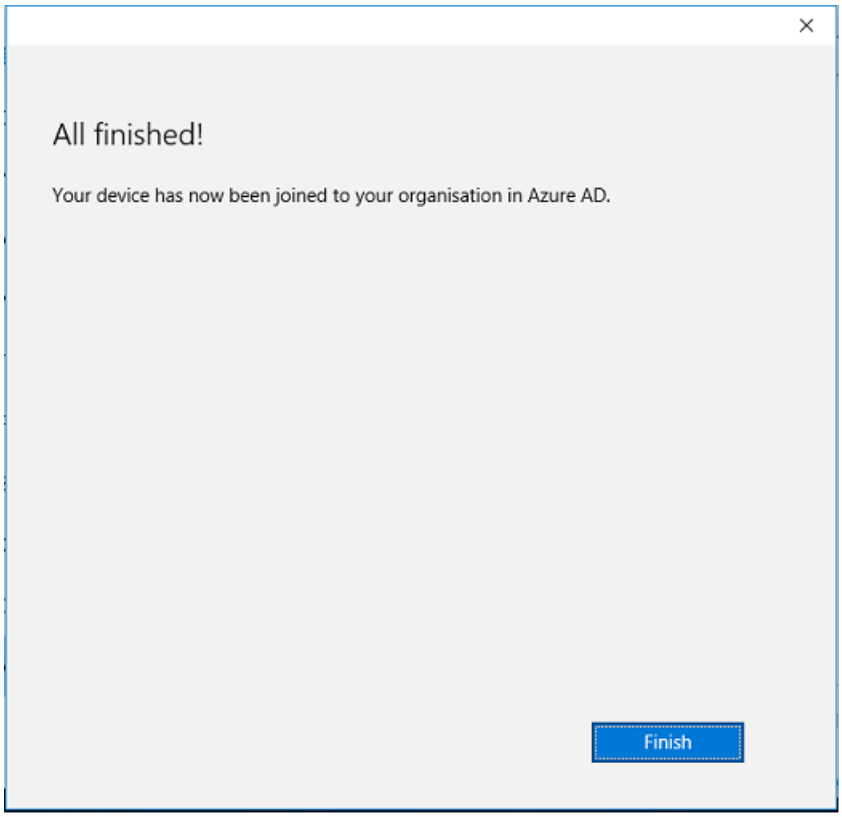

Der UPN muss mit dem von dem AD FS-Domänencontroller erkannten UPN übereinstimmen.





© 1999-2017 Citrix Systems, Inc. All rights reserved.




Prüfen Sie den Erfolg der Azure AD-Einbindung, indem Sie die Maschine neu starten und sich mit der E-Mail-Adresse des Benutzers anmelden. Nach der Anmeldung starten Sie Microsoft Edge und stellen Sie eine Verbindung mit http://myapps.microsoft.com her. Die Website müsste Single Sign-On automatisch verwenden.

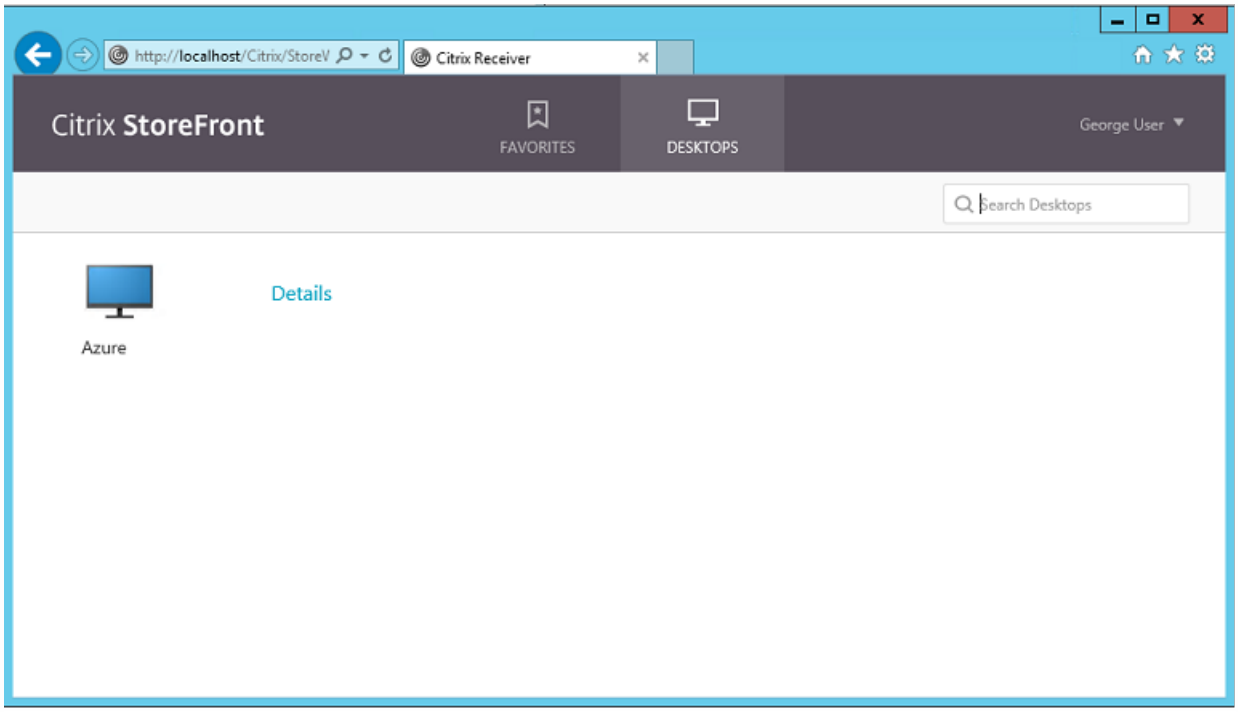
# Installieren von XenApp oder XenDesktop

Sie können die virtuellen Maschinen für Delivery Controller und VDA in Azure direkt vom XenApp- bzw. XenDesktop-ISO-Image normal installieren.

In diesem Beispiel wird StoreFront auf demselben Server wie der Delivery Controller installiert. Der VDA wird als eigenständiger Windows 2012 R2 RDS-Worker ohne Integration in Maschinenerstellungsdienste installiert (optional könnte dies aber konfiguriert werden). Vergewissern Sie sich bevor Sie fortfahren, dass der Benutzer George@citrixsamldemo.net

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

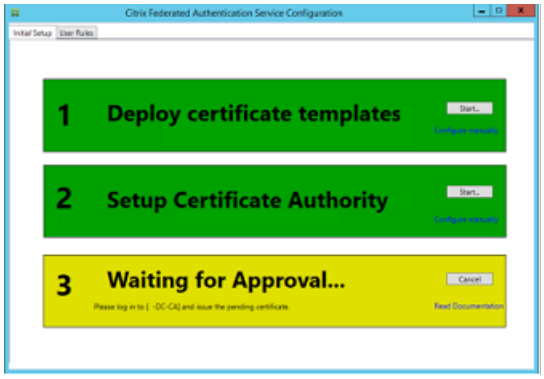
sich mit einem Kennwort authentifizieren kann.




Führen Sie das PowerShell-Cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** auf dem Controller aus, damit StoreFront eine Authentifizierung ohne Anmeldeinformationen des Benutzers durchführen kann.

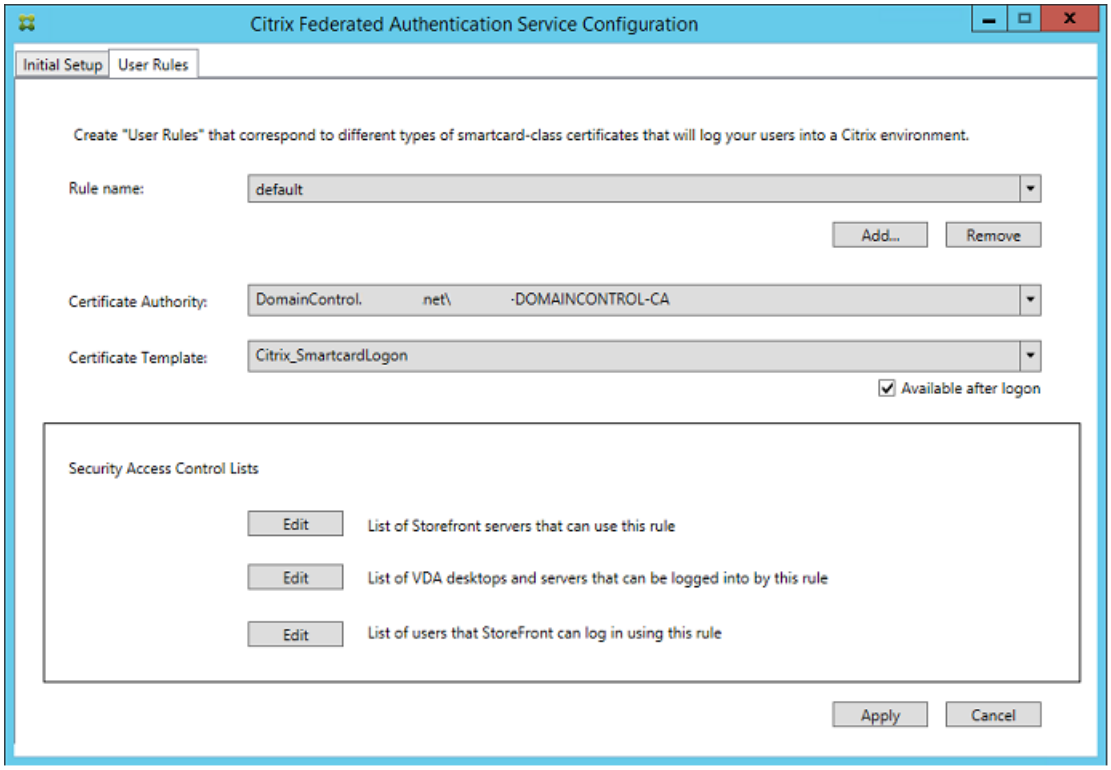
**Installieren des Verbundauthentifizierungsdiensts**

Installieren Sie die Komponente Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) auf dem AD FS-Server und konfigurieren Sie eine Regel, durch die der Controller als vertrauenswürdige StoreFront agiert.



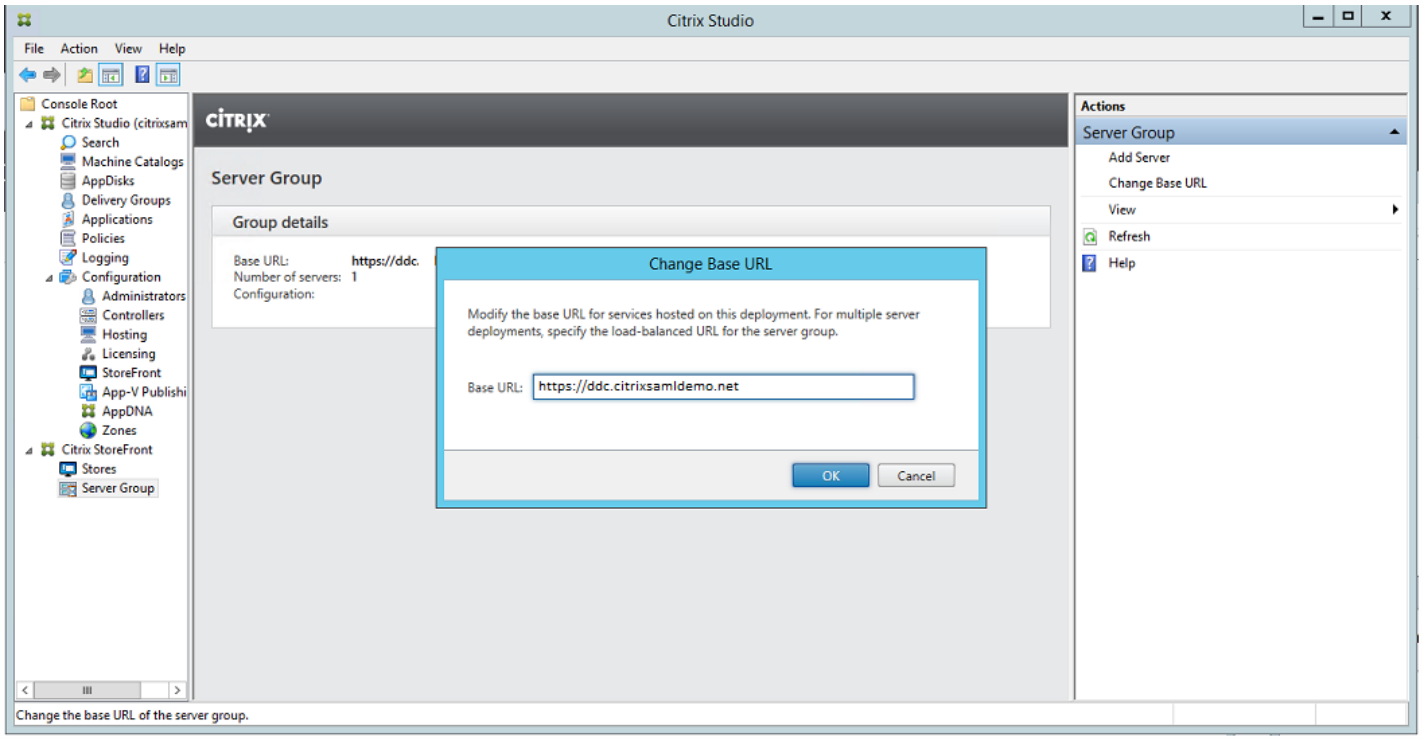


© 1999-2017 Citrix Systems, Inc. All rights reserved.




### Konfigurieren von StoreFront

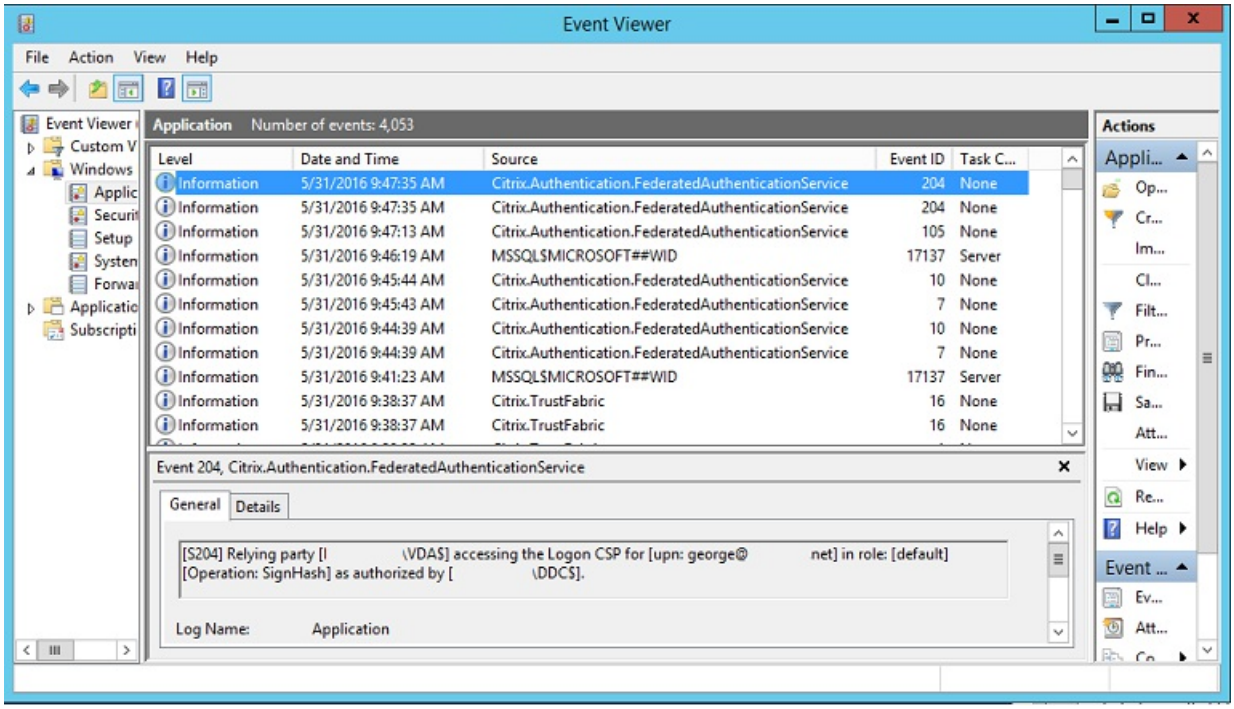
Fordern Sie ein Computerzertifikat für den Delivery Controller an und konfigurieren Sie IIS und StoreFront für HTTPS, indem Sie eine IIS-Bindung für Port 443 festlegen und die StoreFront-Basisadresse in "https:" ändern.




Konfigurieren Sie StoreFront für die Verwendung des FAS-Servers (mit dem PowerShell-Skript aus dem Artikel

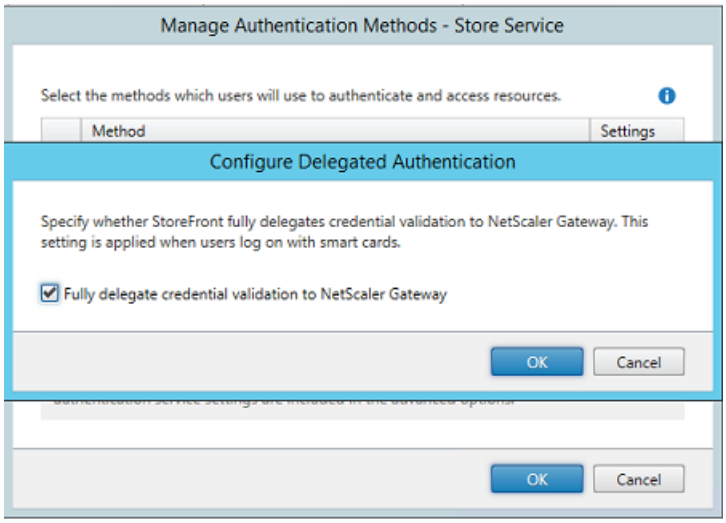

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verbundauthentifizierungsdienst) und führen Sie Azure-intern einen Test durch. Vergewissern Sie sich dabei, dass die Anmeldung über FAS geht, indem Sie die Ereignisanzeige des FAS-Servers prüfen.



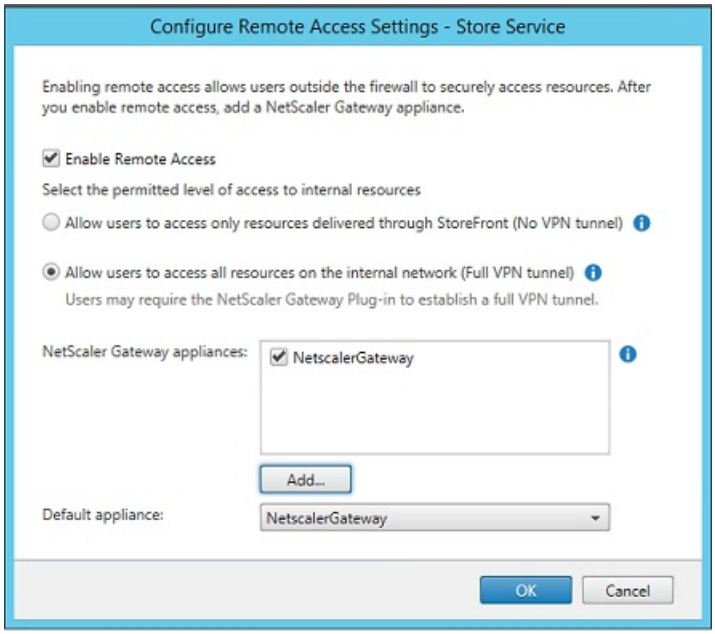

**Konfigurieren von StoreFront zur Verwendung von NetScaler**

Konfigurieren Sie im Bereich **Authentifizierungsmethoden verwalten** der StoreFront-Verwaltungskonsole StoreFront für die Authentifizierung über NetScaler.



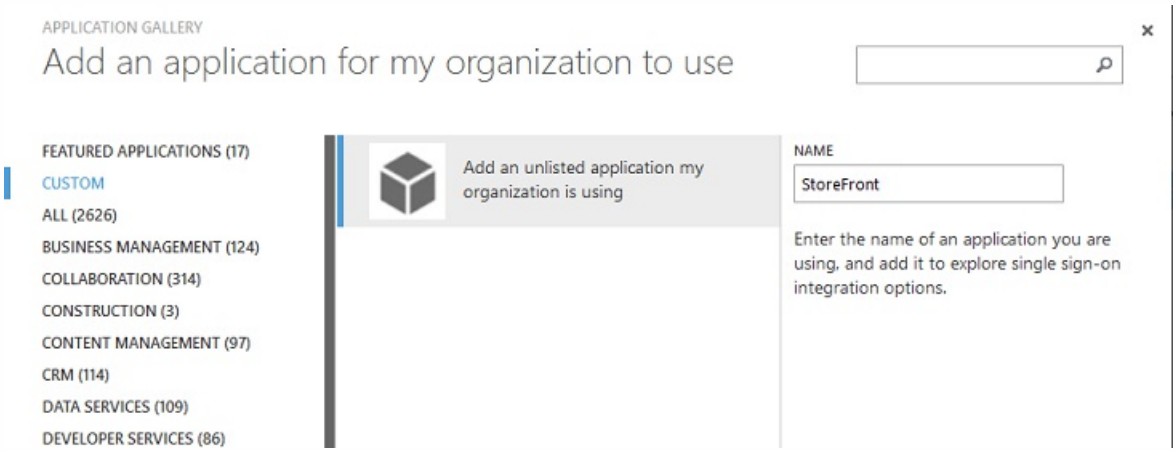

Zum Integrieren der NetScaler-Authentifizierungsoptionen konfigurieren Sie eine Secure Ticket Authority (STA) und konfigurieren Sie die NetScaler Gateway-Adresse.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Konfigurieren einer neuen Azure-Anwendung für das Single Sign-On bei StoreFront

In diesem Abschnitt werden die Single Sign-On-Features von Azure AD SAML 2.0 verwendet, die zurzeit ein Azure AD-Premium-Abonnement erfordern. Wählen Sie in der Azure AD-Verwaltung **Neue Anwendung** und **Anwendung aus dem Katalog hinzufügen**.




Wählen Sie **BENUTZERDEFINIERT > Eine nicht aufgeführte von meiner Organisation eingesetzte Anwendung hinzufügen**, um eine neue benutzerdefinierte Anwendung für die Benutzer zu erstellen.

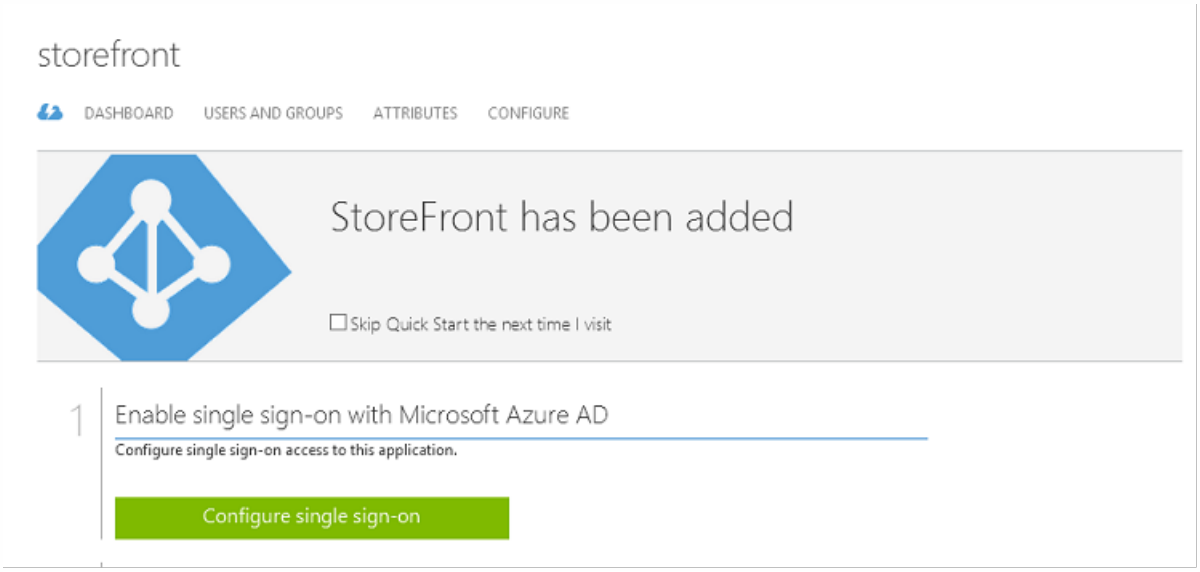
**Konfigurieren eines Symbols**

Erstellen Sie ein Bild einer Größe von 215 x 215 Pixel und laden Sie es auf der Seite KONFIGURIEREN zur Verwendung als Symbol für die Anwendung hoch.

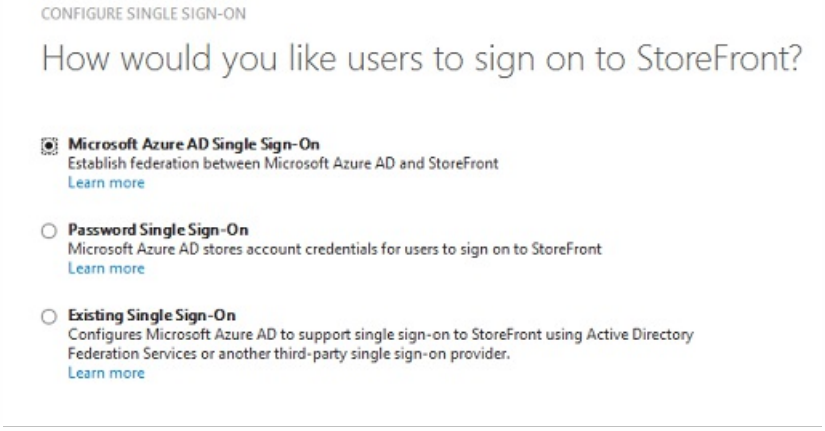

© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Konfigurieren der SAML-Authentifizierung**

Kehren Sie auf die Dashboard-Übersichtsseite zurück und wählen Sie **Single Sign-On konfigurieren**.



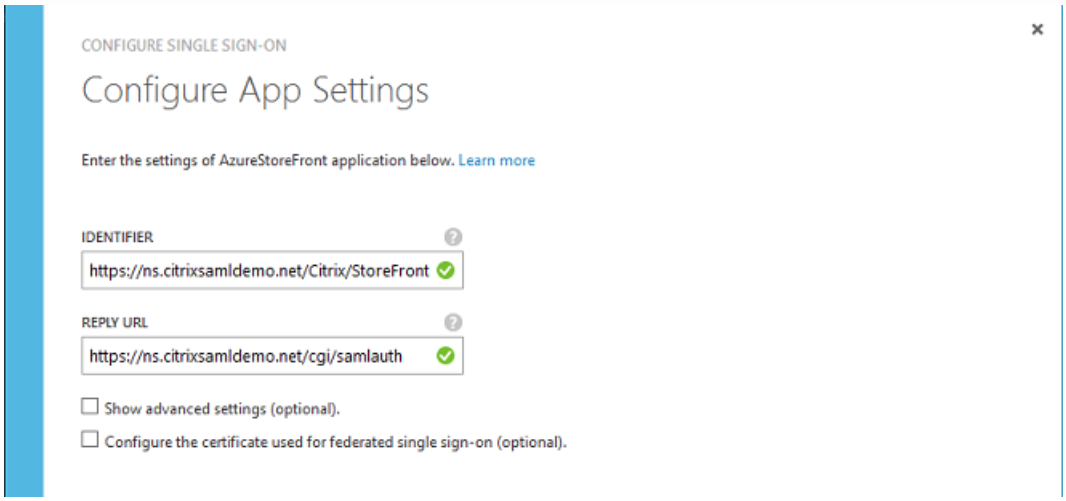

In dieser Bereitstellung wird die SAML 2.0-Authentifizierung verwendet. Dies entspricht Single Sign-On in Microsoft Azure AD.



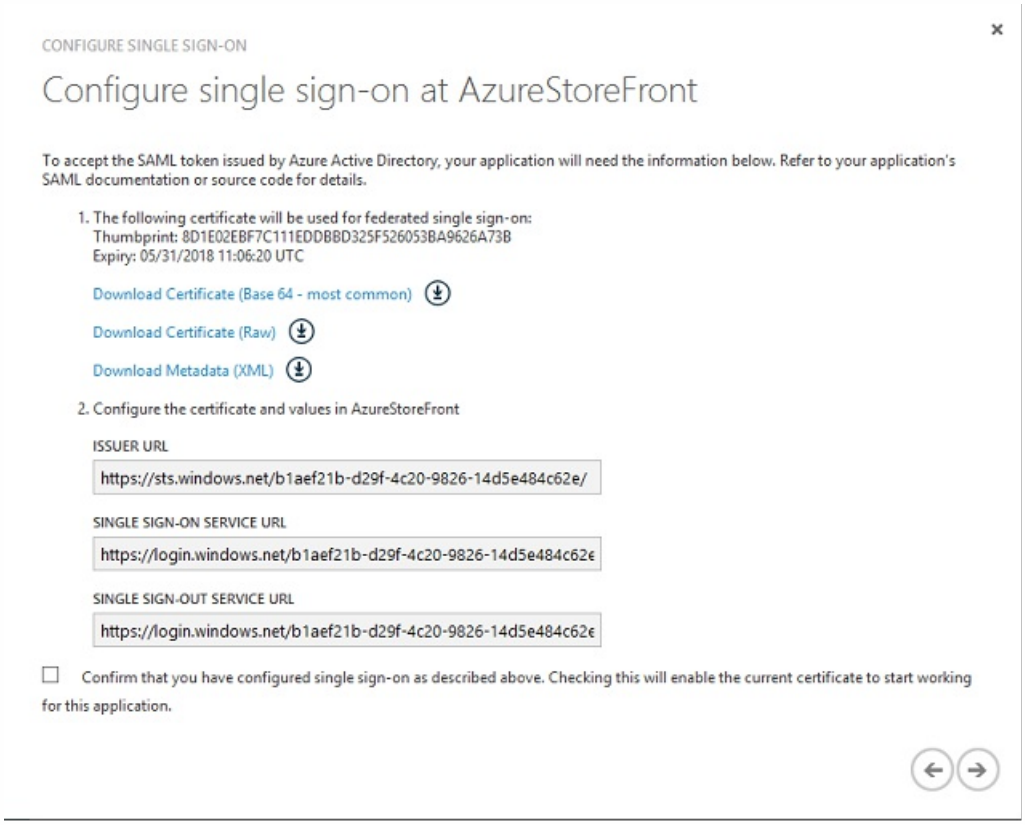


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Kennung darf eine beliebige Zeichenfolge sein (sie muss mit der für NetScaler bereitgestellten Konfiguration übereinstimmen). Im vorliegenden Beispiel ist die Antwort-URL "/cgi/samlauth" auf dem NetScaler-Server.




Die nächste Seite enthält Informationen zum Konfigurieren von NetScaler als vertrauende Seite für Azure AD.

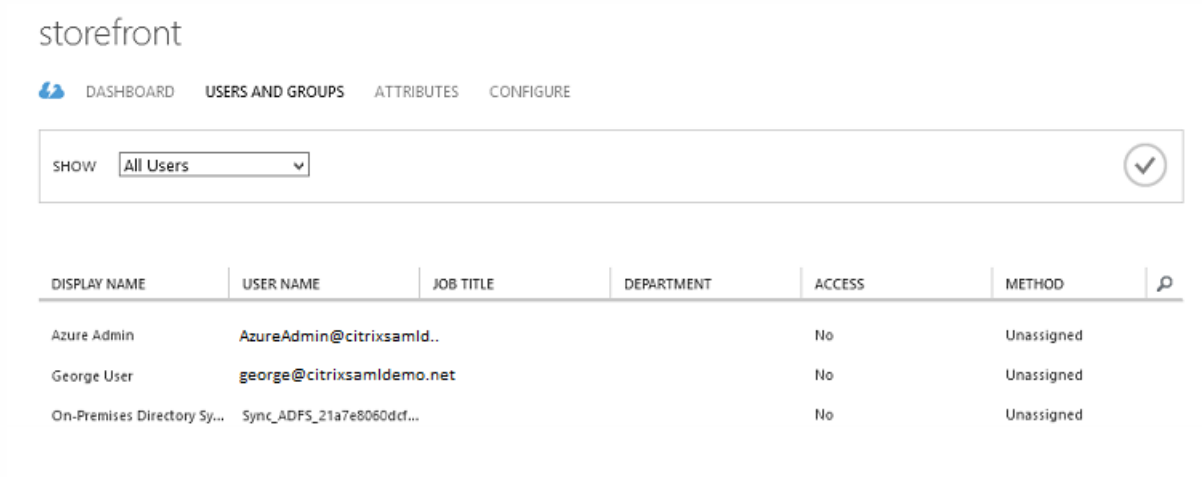



Laden Sie das vertrauenswürdige Base-64-Signaturzertifikat herunter und kopieren Sie die Sign-On- und die Sign-Out-URL. Diese fügen Sie später in die Bildschirme zur NetScaler-Konfiguration ein.

**Zuweisen der Anwendung zu Benutzern**

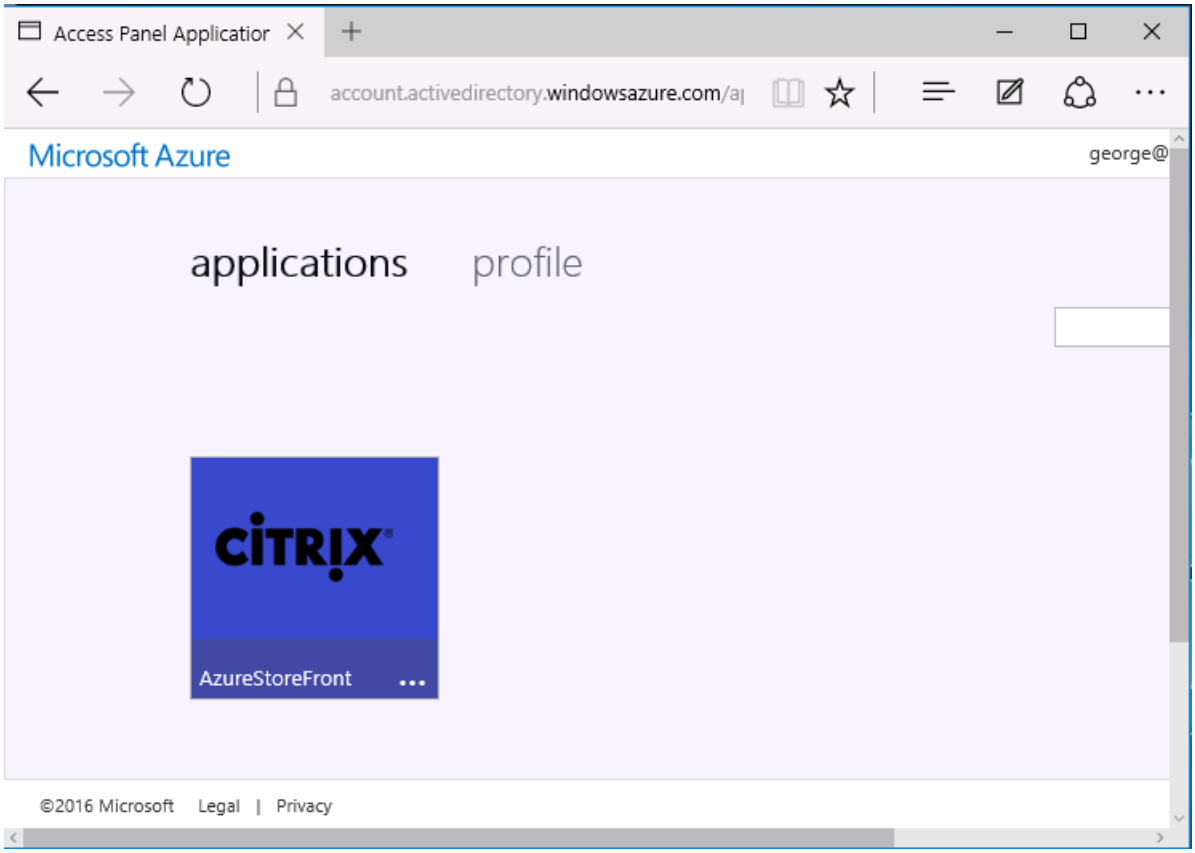

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Der letzte Schritt besteht in der Aktivierung der Anwendung, damit sie für die Benutzer auf der Steuerungsseite "myapps.microsoft.com" angezeigt wird. Dafür wird die Seite BENUTZER UND GRUPPEN verwendet. Weisen Sie Zugriff für die über Azure AD Connect synchronisierten Domänenbenutzerkonten zu. Andere Konten können ebenfalls verwendet werden, sie müssen jedoch explizit zugeordnet werden, da sie nicht dem Muster @ entsprechen.




**Seite "MyApps"**

Wenn die Anwendung konfiguriert wurde, wird sie in der Azure-Anwendungsliste angezeigt, wenn die Benutzer https://myapps.microsoft.com besuchen.

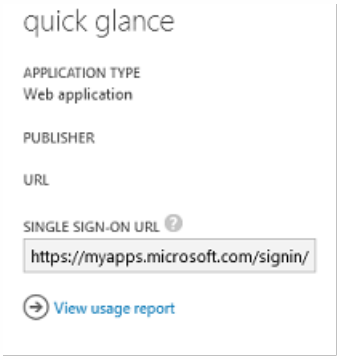



Wenn Windows 10 Azure AD beigetreten ist, unterstützt es Single Sign-On für Azure-Anwendungen. Bei einem Klick auf das Symbol wird der Browser an die zuvor konfigurierte SAML-Webseite cgi/samlauth umgeleitet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**URL für Single Sign-On**

Kehren Sie zu der Anwendung im Azure AD-Dashboard zurück. Es gibt jetzt eine Single Sign-On-URL für die Anwendung. Diese URL wird zur Erstellung von Browserlinks und Startmenüverknüpfungen verwendet, die die Benutzer direkt an StoreFront umleiten.




Fügen Sie diese URL in einen Webbrowser ein, um sicherzustellen, dass Sie von Azure AD an die zuvor konfigurierte NetScaler-Webseite cgi/samlauth umgeleitet werden. Dies funktioniert nur dann, wenn ein Benutzer zugewiesen wurde, zudem ist Single Sign-On nur bei Anmeldungssitzungen möglich, wenn Windows 10 Azure AD beigetreten ist. (Andere Benutzer werden aufgefordert, ihre Azure AD-Anmeldeinformationen einzugeben.)

# Installieren und Konfigurieren von NetScaler Gateway

Für den Remote-Zugriff auf die Bereitstellung wird in diesem Beispiel eine separate VM mit NetScaler verwendet. Diese kann im Azure-Store erworben werden. In diesem Beispiel wird die "Bring your own License"-Lizenzversion für NetScaler 11.0 verwendet.

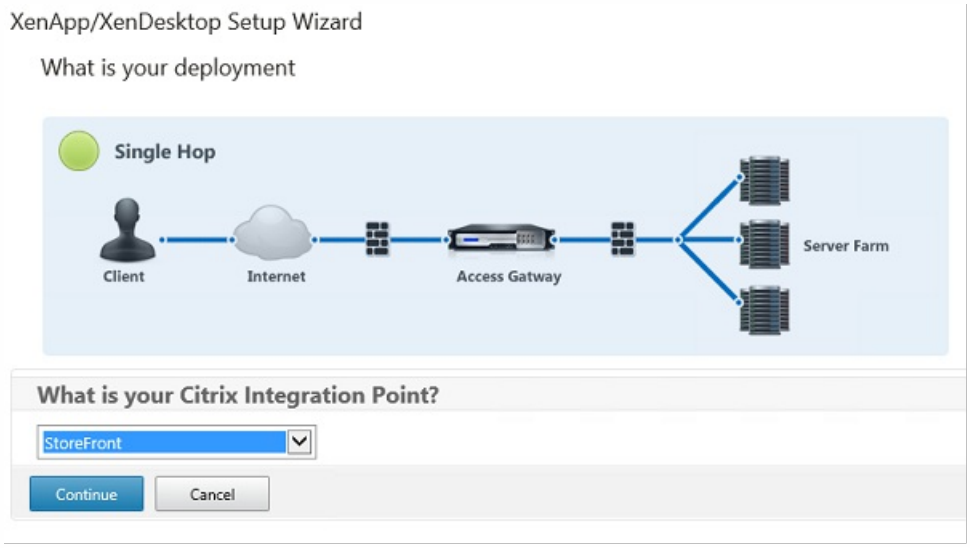
 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Melden Sie sich bei der NetScaler-VM an, indem Sie im Webbrowser die interne IP-Adresse und die bei der Benutzerauthentifizierung angegebenen Anmeldeinformationen eingeben. Sie müssen das Kennwort des nsroot-Benutzers in einer Azure AD-VM ändern.

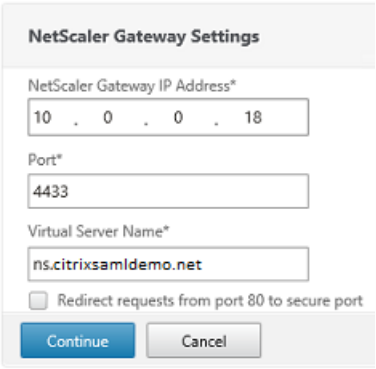
Fügen Sie Lizenzen hinzu (führen Sie nach dem Hinzufügen jeder Lizenz einen Neustart durch) und verweisen Sie die DNS-Auflösung an den Microsoft-Domänencontroller.

**Ausführen des XenApp- und XenDesktop-Setupassistenten**

In diesem Beispiel wird zunächst eine einfache StoreFront-Integration ohne SAML konfiguriert. Wenn diese Bereitstellung betriebsbereit ist, wird eine SAML-Anmelderichtlinie hinzugefügt.

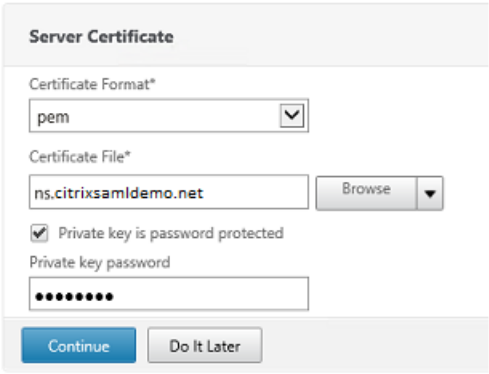



Wählen Sie die standardmäßigen NetScaler-StoreFront-Einstellungen. Zur Verwendung in Microsoft Azure wird in diesem Beispiel Port 4433 anstelle von Port 443 konfiguriert. Alternativ können Sie eine Portweiterleitung einrichten oder die Zuweisung der Verwaltungswebsite von NetScaler ändern.



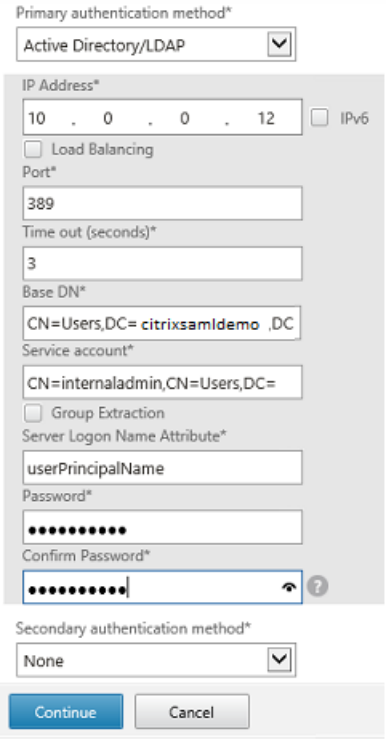

Der Einfachheit halber wird in diesem Beispiel ein in einer Datei gespeichertes, vorhandenes Serverzertifikat mit privatem Schlüssel hochgeladen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Konfigurieren des Domänencontrollers für die AD-Kontoverwaltung**

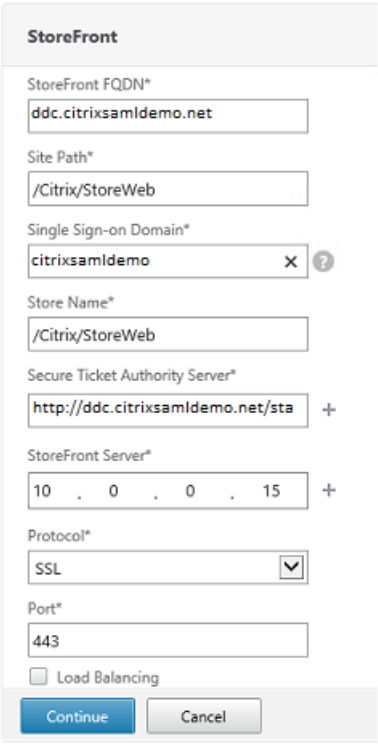
Der Domänencontroller wird zur Kontoauflösung verwendet. Fügen Sie daher seine IP-Adresse in die primäre Authentifizierungsmethode ein. Beachten Sie die in den einzelnen Feldern im Dialogfeld erforderlichen Formate.




# Konfigurieren der StoreFront-Adresse

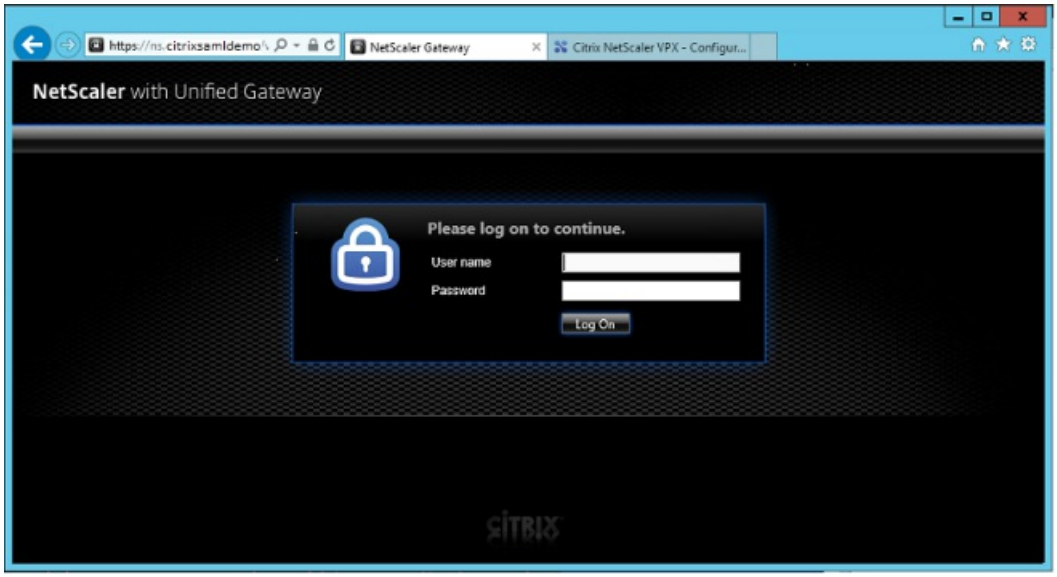
In diesem Beispiel wurde StoreFront für HTTPS konfiguriert. Wählen Sie daher die SSL-Protokolloptionen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Prüfen der NetScaler-Bereitstellung**

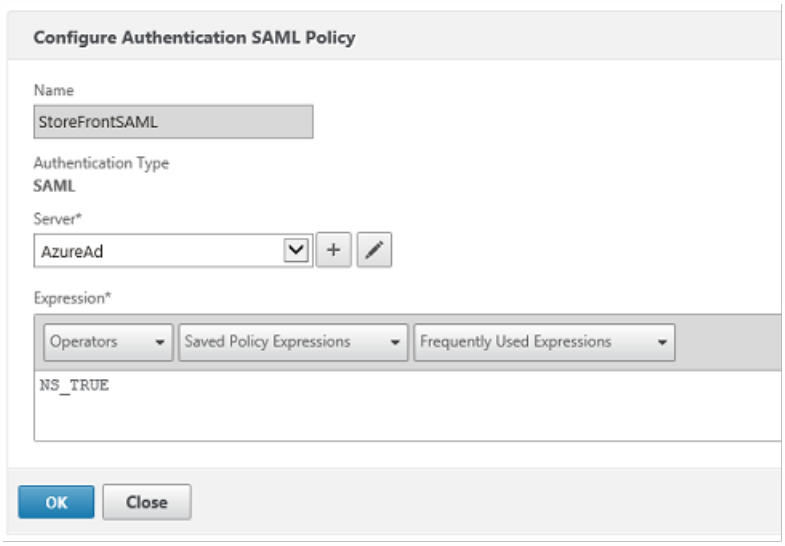
Stellen Sie eine Verbindung mit NetScaler her und überprüfen Sie, ob Authentifizierung und Start mit den Anmeldeinformationen funktionieren.



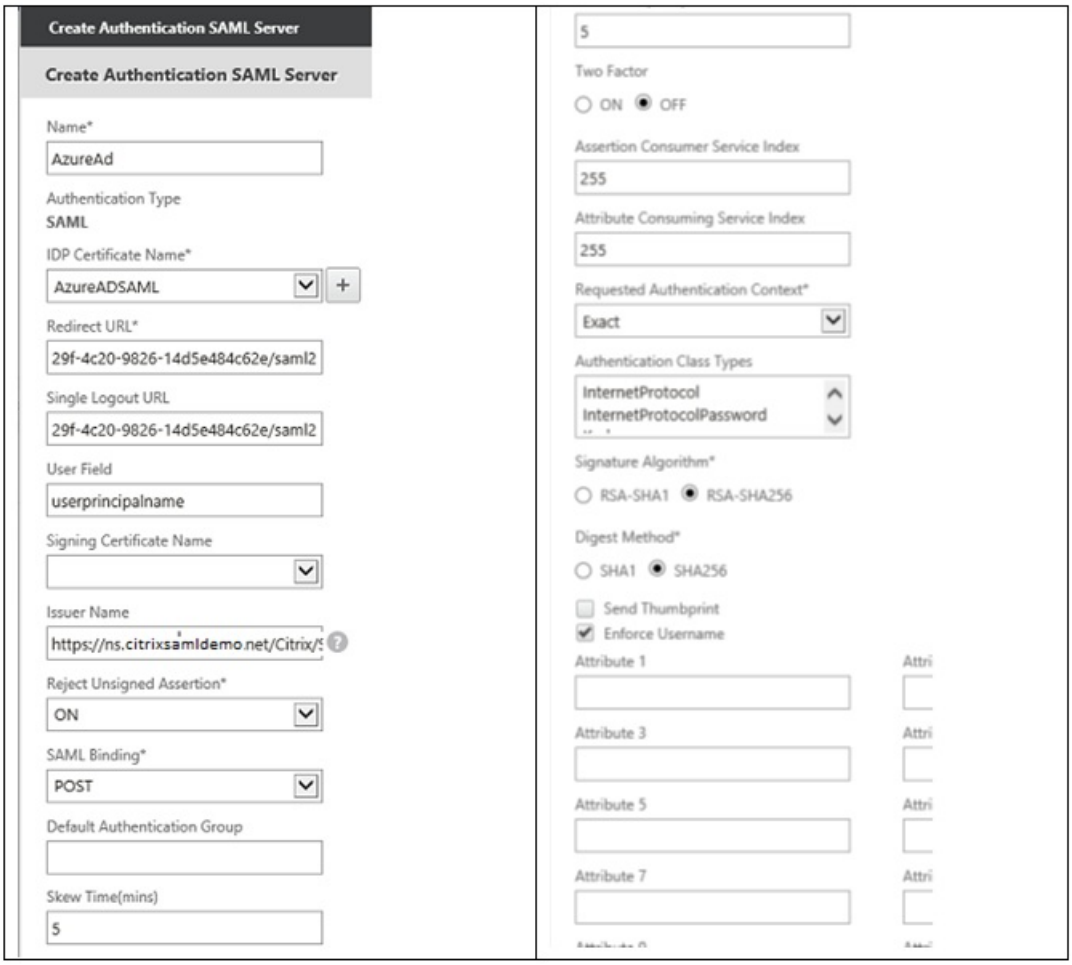

# Aktivieren der Unterstützung für die NetScaler-SAML-Authentifizierung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Verwendung von SAML bei StoreFront ähnelt der Verwendung von SAML für andere Websites. Fügen Sie eine neue SAML-Richtlinie mit dem Ausdruck **NS_TRUE** hinzu.




Konfigurieren Sie den neuen SAML-IdP-Server mit den zuvor von Azure AD erhaltenen Informationen.



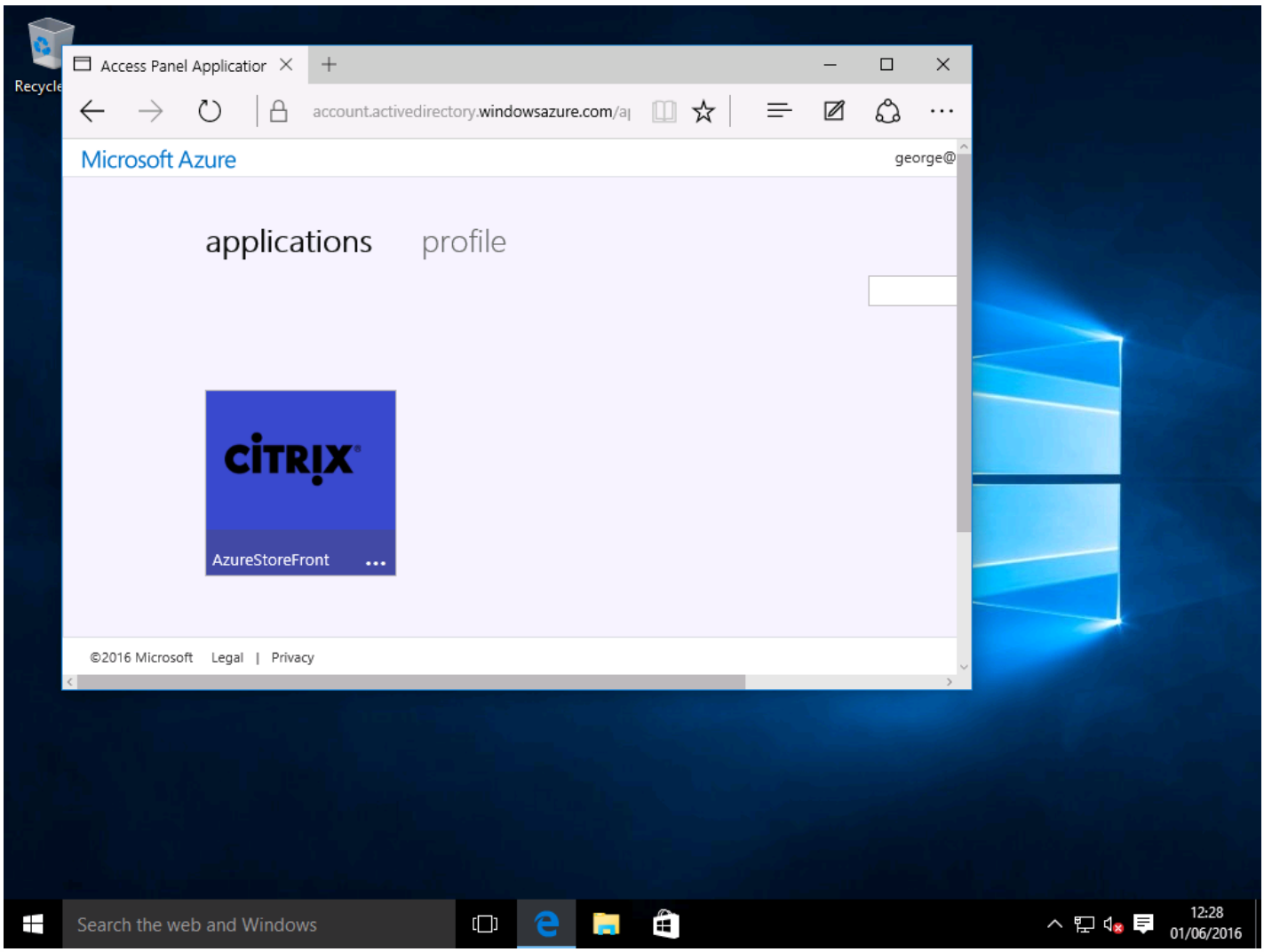


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überprüfen des Gesamtsystems

Melden Sie sich bei einem Azure AD beigetretenen Windows 10-Desktop mit einem in Azure AD registrierten Konto an. Starten Sie Microsoft Edge und stellen Sie eine Verbindung mit https://myapps.microsoft.com her.

Im Webbrowser müssten nun die Azure AD-Anwendungen für den Benutzer angezeigt werden.




Vergewissern Sie sich, dass bei einem Klick auf das Symbol eine Umleitung an einen authentifizierten StoreFront-Server erfolgt.

Prüfen Sie außerdem, ob bei direkten Verbindungen mit der Single Sign-On-URL und mit der NetScaler-Site eine Umleitung an Microsoft Azure und zurück stattfindet.

Vergewissern Sie sich zuletzt, dass dieselben URLs auch bei nicht Azure AD beigetretenen Maschinen funktionieren (allerdings ist hier bei der ersten Verbindung ein Sign-On bei Azure AD erforderlich).

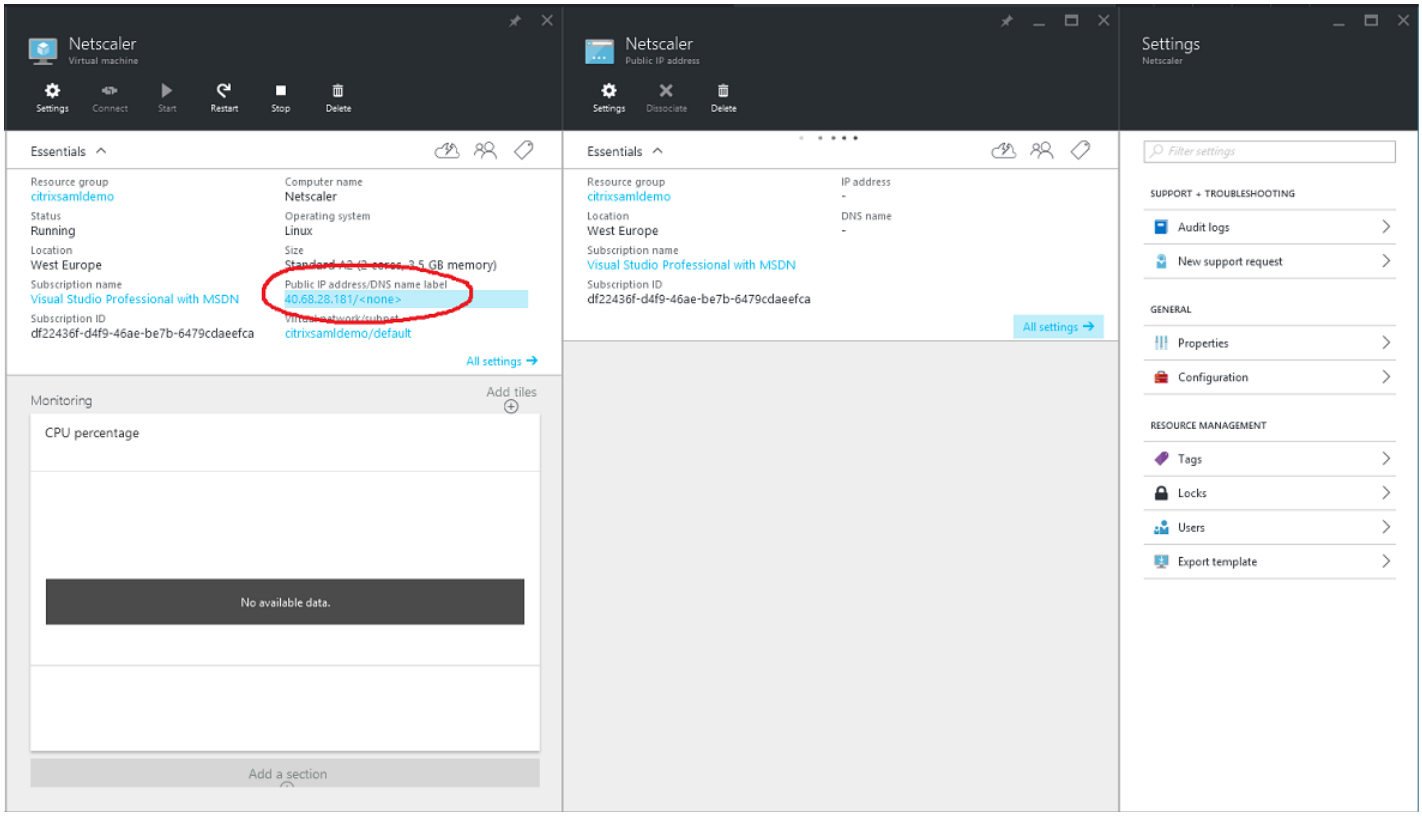
# Anhang


© 1999-2017 Citrix Systems, Inc. All rights reserved.

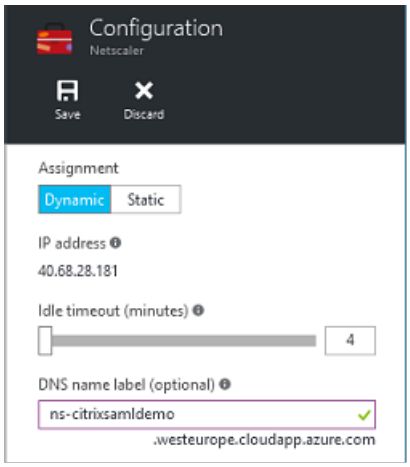
Wenn Sie eine VM in Azure einrichten, müssen verschiedene Standardoptionen konfiguriert werden.

**Angeben einer öffentlichen IP-Adresse und einer DNS-Adresse**

Azure weist allen VMs eine IP-Adresse im internen Subnetz zu (in diesem Beispiel 10.*.*.*). Standardmäßig wird auch eine öffentliche IP-Adresse angegeben, auf die durch eine dynamisch aktualisierte DNS-Bezeichnung verwiesen werden kann.




Wählen Sie **Configuration** für **Public IP address/DNS name label**. Wählen Sie eine öffentliche DNS-Adresse für die VM. Diese kann für CNAME-Verweise in anderen DNS-Zonendateien verwendet werden, damit alle DNS-Einträge richtig auf die VM verweisen, selbst wenn die IP-Adresse neu zugewiesen wird.

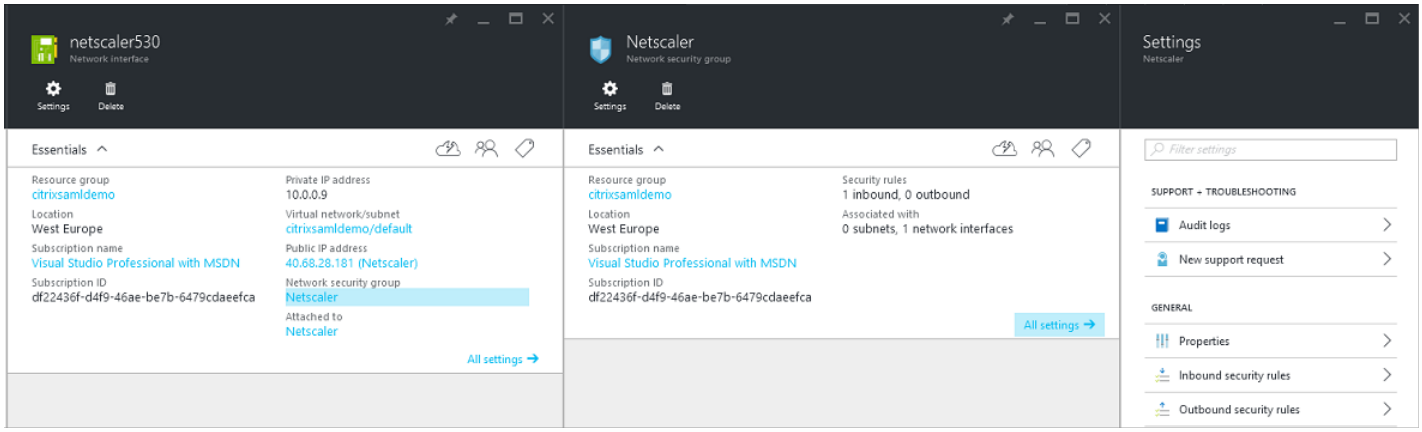



**Einrichten von Firewallregeln (Sicherheitsgruppe)**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Auf jede VM in einer Cloud werden automatisch einige Firewallregeln angewendet, die als Sicherheitsgruppe bezeichnet werden. Die Sicherheitsgruppe steuert den Datenverkehr von der öffentlichen an die private IP-Adresse. Standardmäßig lässt Azure die RDP-Weiterleitung an alle VMs zu. Der NetScaler- und der AD FS-Server müssen ebenfalls TLS-Datenverkehr (443) weiterleiten.

Öffnen Sie **Network Interfaces** für eine VM und klicken Sie dann auf **Network Security Group**. Konfigurieren Sie **Inbound security rules** zum Zulassen des erforderlichen Datenverkehrs im Netzwerk.




# Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts

Aug 17, 2016

Die folgenden Artikel enthalten Anweisungen für die Konfiguration und Verwaltung des Verbundauthentifizierungsdiensts (FAS):

- Schutz privater Schlüssel
- Konfiguration der Zertifizierungsstelle
- Sicherheits- und Netzwerkverwaltung
- Problembehandlung von Windows-Anmeldeproblemen
- Cmdlet-Hilfedateien für das PowerShell SDK

Verwandte Informationen

- Primäre Referenz für die Installation und anfängliche Einrichtung des FAS ist der Artikel Verbundauthentifizierungsdienst.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichsten FAS-Architekturen sowie Links zu Artikeln über komplexere Architekturen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfiguration einer Zertifizierungsstelle für den Verbundauthentifizierungsdienst

Jul 13, 2016

Dieser Abschnitt beschreibt die erweiterte Konfiguration des Citrix Verbundauthentifizierungsdiensts (Federated Authentication Service, FAS) für die Integration mit Zertifizierungsstellenservern, die nicht von der FAS-Verwaltungskonsole unterstützt werden. In den Anweisungen werden PowerShell-APIs verwendet, die der Verbundauthentifizierungsdienst bietet. Grundlegende Kenntnisse von PowerShell werden für die Ausführung der Anweisungen in diesem Abschnitt vorausgesetzt.

# Einrichten mehrerer Zertifizierungsstellenserver für die Verwendung im FAS

In diesem Abschnitt wird beschrieben, wie Sie einen FAS-Server so einrichten, dass mehrere Zertifizierungsstellenserver Zertifikate ausstellen können. Dies ermöglicht Lastausgleich und Failover für die Zertifizierungsstellenserver.

**Schritt 1: Bestimmen, wie viele Zertifizierungsstellenserver der FAS finden kann**

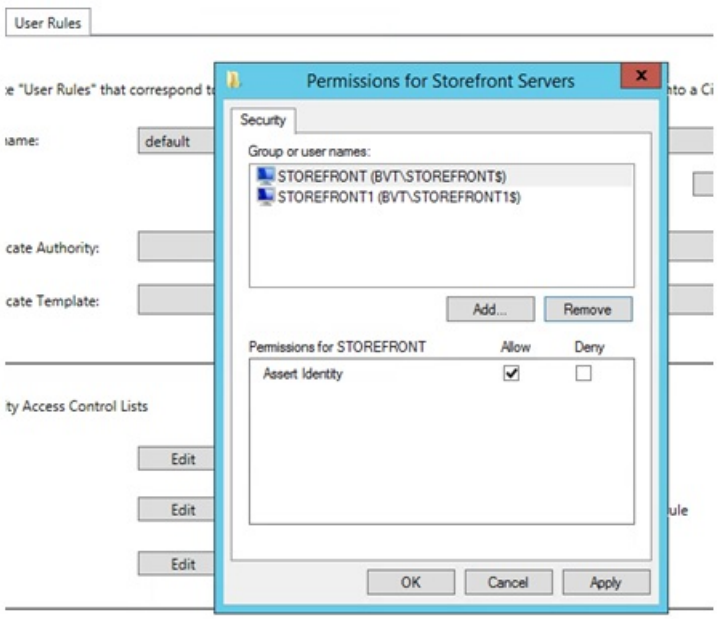
Bestimmen Sie mit dem Cmdlet Get-FASMsCertificateAuthority, mit welchen Zertifizierungsstellenservern FAS eine Verbindung herstellen kann. Das folgende Beispiel zeigt, dass FAS mit drei Zertifizierungsstellenservern eine Verbindung herstellen kann.

```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                                IsDefault PublishedTemplates
-------                                --------- ------------------
DC1.bvt.local\bvt-DC1-CA                   False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
```

**Schritt 2: Ändern der vorhandenen Zertifikatdefinition**

Citrix empfiehlt, dass Sie mit der FAS-Verwaltungskonsole (und nicht mit PowerShell) eine Rolle erstellen. Auf diese Weise müssen Sie den SDL nicht später manuell hinzufügen. Im folgenden Beispiel wird eine Rolle namens "Default" erstellt, in der die Zugriffsregel konfiguriert ist:

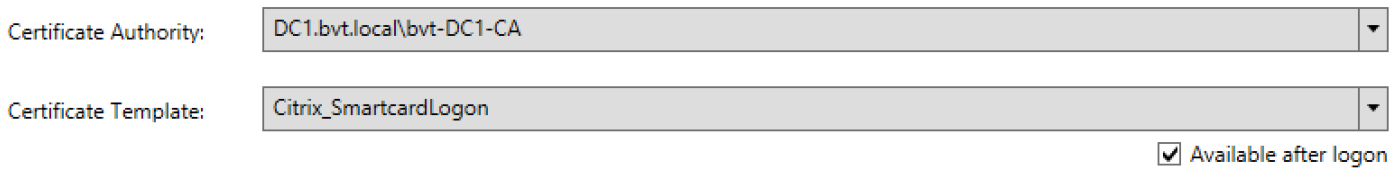

© 1999-2017 Citrix Systems, Inc. All rights reserved.




Sie müssen die Zertifikatdefinition konfigurieren, damit Sie mehrere Zertifizierungsstellen im Feld für die Zertifizierungsstelle hinzufügen können (wird in diesem Release nicht unterstützt). Als Erstes benötigen Sie den Namen der Zertifikatdefinition. Der Name kann nicht mit der Verwaltungskonsole ermittelt werden. Verwenden Sie zur Ermittlung das Cmdlet Get-FASCertificateDefinition.

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

Auf der Benutzeroberfläche sieht dies wie folgt aus:




Wenn Sie den Namen der Zertifikatdefinition ermittelt haben, ändern Sie die Zertifikatdefinition, damit Sie eine Liste mit Zertifizierungsstellen haben:

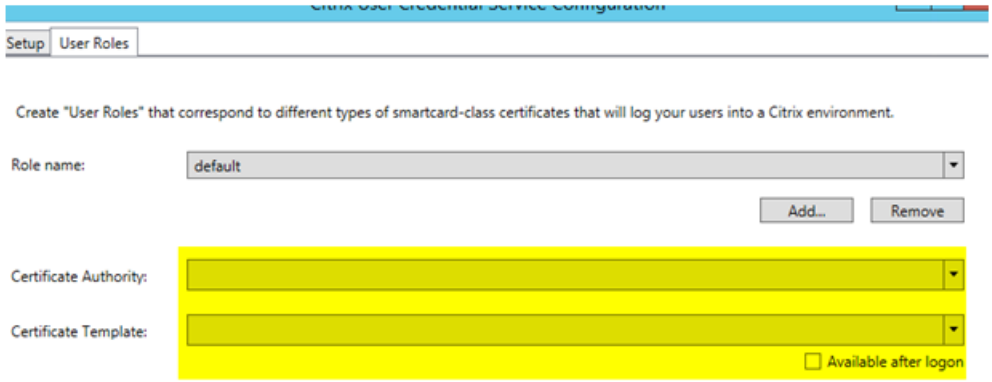
```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Das Cmdlet Get-FASCertificateDefinition gibt nun Folgendes zurück:

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

**Hinweis:** Nach diesem Vorgang ist die FAS-Verwaltungskonsole nicht funktionsfähig. Beim Laden wird in "Certificate Authority" und "Certificate Template" ein leeres Feld angezeigt:




FAS funktioniert jedoch noch völlig normal. Wenn Sie mit der Konsole die Zugriffsregel ändern, wiederholen Sie Schritt 2, um alle Zertifizierungsstellen anzuzeigen.

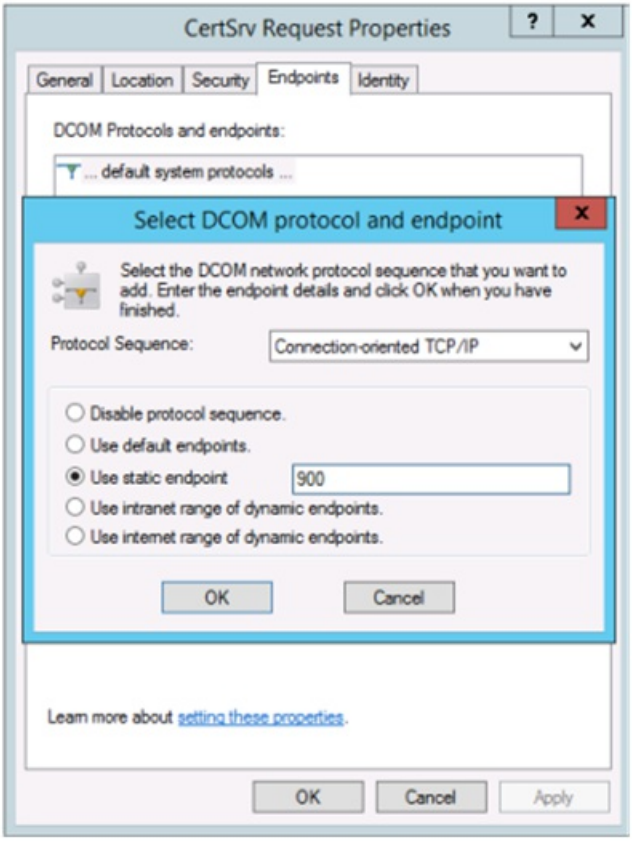
**Erwartete Verhaltensänderungen**

Wenn Sie den FAS-Server mit mehreren Zertifizierungsstellenservern konfiguriert haben, wird die Generierung von Benutzerzertifikaten auf alle konfigurierten Zertifizierungsstellenserver verteilt. Wenn einer der konfigurierten Zertifizierungsstellenserver ausfällt, wechselt der FAS-Server zu einem anderen verfügbaren Zertifizierungsstellenserver.

# Konfigurieren der Microsoft-Zertifizierungsstelle für TCP-Zugriff

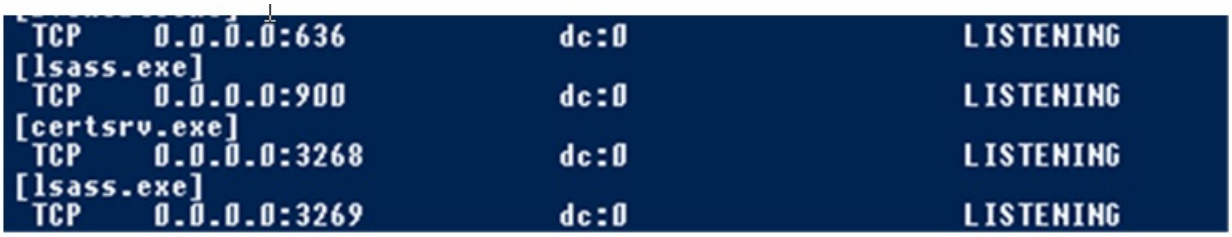
Standardmäßig verwendet die Microsoft-Zertifizierungsstelle für den Zugriff DCOM. Beim Implementieren von Firewallsicherheit kann dies sehr komplex sein, daher bietet Microsoft die Möglichkeit, zu einem statischen TCP-Port zu wechseln. Öffnen Sie auf der Microsoft-Zertifizierungsstelle den DCOM-Konfigurationsbereich und bearbeiten Sie die Eigenschaften der DCOM-Anwendung "CertSrv Request":


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Ändern Sie die Endpunkte, indem Sie einen statischen Endpunkt auswählen, und geben Sie eine TCP-Portnummer ein (900 in der Abbildung oben).

Starten Sie die Microsoft-Zertifizierungsstelle neu und senden Sie eine Zertifikatanforderung. Wenn Sie "netstat –a –n –b" ausführen, sollte certsrv zur Überwachung Port 900 verwenden:




Sie brauchen den FAS-Server (bzw. andere Maschinen, die die Zertifizierungsstelle verwenden) nicht zu konfigurieren, da DCOM durch Verwendung des RPC-Ports eine Aushandlungsphase hat. Wenn ein Client DCOM verwenden muss, stellt er eine Verbindung zum DCOM RPC-Dienst auf dem Zertifikatserver her und fordert Zugriff auf einen bestimmten DCOM-Server an. Dadurch wird Port 900 geöffnet und der DCOM-Server gibt dem FAS-Server Anweisungen zum Herstellen der Verbindung.

# Vorabgenerieren von Benutzerzertifikaten

Die Anmeldung erfolgt für Benutzer erheblich schneller, wenn Benutzerzertifikate im FAS-Server vorab generiert werden. In


© 1999-2017 Citrix Systems, Inc. All rights reserved.

den folgenden Abschnitten wird die erforderliche Vorgehensweise für einen oder mehrere FAS-Server beschrieben.

### Abrufen einer Liste der Active Directory-Benutzer

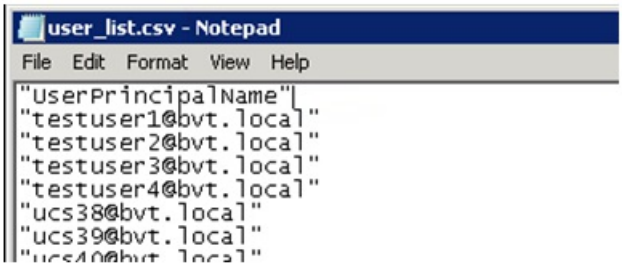
Sie können die Zertifikatgenerierung verbessern, indem Sie eine Liste der Benutzer von Active Directory abrufen und als Datei (z. B. als CSV-Datei) speichern, wie im folgenden Beispiel dargestellt.

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

if ($searchbase –ne “”) {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," 
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

Get-ADUser ist ein Standardcmdlet zum Abrufen einer Liste der Benutzer. Das obige Beispiel enthält ein Filterargument, damit nur Benutzer mit einem UserPrincipalName aufgelistet werden, deren Kontostatus "enabled" ist.

Mit dem Argument SearchBase können Sie den Teil von Active Directory einschränken, der nach Benutzern durchsucht wird. Wenn Sie alle Benutzer in AD durchsuchen möchten, lassen Sie das Argument aus. Hinweis: Die Abfrage gibt u. U. eine große Anzahl Benutzer zurück.

Die CSV-Datei sieht wie folgt aus:




### FAS-Server

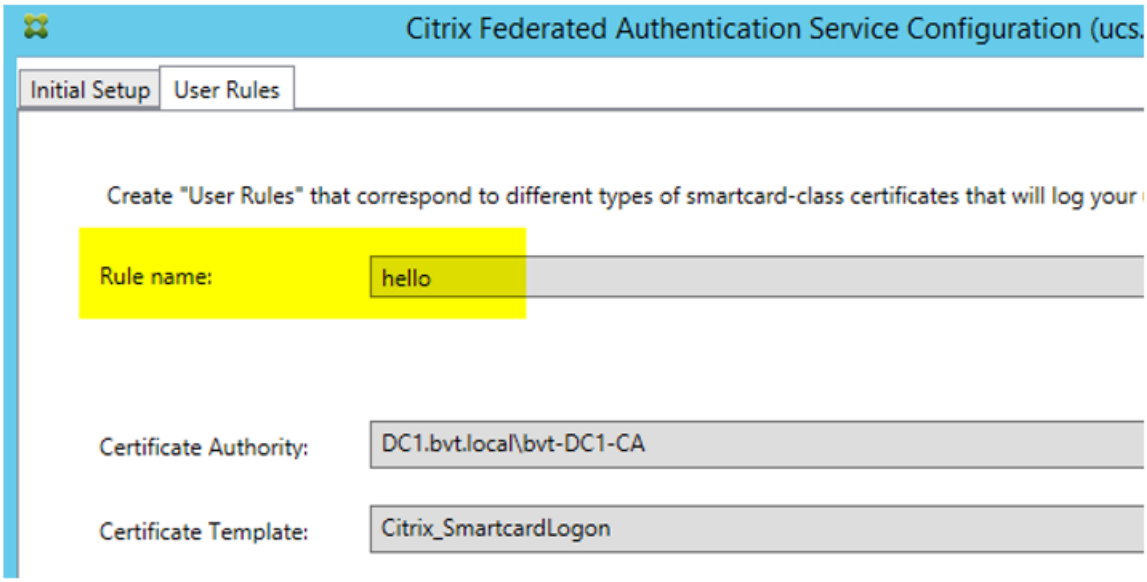
Das folgende PowerShell-Skript erstellt mit der generierten Benutzerliste eine Liste mit Benutzerzertifikaten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ) {
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ) {
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

Wenn Sie mehr als einen FAS-Server haben, wird das Zertifikat für einen bestimmten Benutzer zweimal generiert: eins auf dem Hauptserver und das andere auf dem Failoverserver.

Das obige Skript wird durch die Regel "default" gesteuert. Wenn Ihre Regel einen anderen Namen hat (z. B. "hello"), ändern Sie im Skript die Variable $rule.




# Erneuern von Registrierungsstellenzertifikaten

Wenn mehrere FAS-Server verwendet werden, können Sie ein FAS-Registrierungsstellenzertifikat erneuern, ohne dass es Auswirkungen auf angemeldete Benutzer hat. Hinweis: Sie können die Autorisierung von FAS auch mit der GUID aufheben


© 1999-2017 Citrix Systems, Inc. All rights reserved.

und FAS neu autorisieren, jedoch werden dabei die FAS-Konfigurationsoptionen zurückgesetzt.

Führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein neues Autorisierungszertifikat:

   New-FasAuthorizationCertificate

2. Notieren Sie die GUID des neuen Autorisierungszertifikats, das mit folgendem Befehl zurückgegeben wird:

   Get-FasAuthorizationCertificate

3. Versetzen Sie den FAS-Server in den Wartungsmodus:

   Set-FasServer –Address -MaintenanceMode $true

4. Wechseln Sie zum neuen Autorisierungszertifikat:

   Set-FasCertificateDefinition –AuthorizationCertificate

5. Heben Sie den Wartungsmodus für den FAS-Server auf:

   Set-FasServer –Address -MaintenanceMode $false

6. Löschen Sie das alte Autorisierungszertifikat:

   Remove-FasAuthorizationCertificate

# Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Schutz durch private Schlüssel beim Verbundauthentifizierungsdienst

Jul 13, 2016

## Einführung

Private Schlüssel werden über das Netzwerkdienstkonto gespeichert und sind standardmäßig als nicht exportierbar markiert.

Es gibt zwei Typen von privaten Schlüsseln:

- Der private Schlüssel des Registrierungsstellenzertifikats (RA-Zertifikat) der Zertifikatvorlage Citrix_RegistrationAuthority.
- Die privaten Schlüssel der Benutzerzertifikate der Zertifikatvorlage Citrix_SmartcardLogon.

Es gibt zwei RA-Zertifikate: Citrix_RegistrationAuthority_ManualAuthorization (24 Stunden gültig) und Citrix_RegistrationAuthority (zwei Jahre gültig).

> Wenn der Administrator während der Ersteinrichtung auf der FAS-Verwaltungskonsole in Schritt 3 auf "Authorize" klickt, generiert der FAS-Server ein Schlüsselpaar und sendet eine Zertifikatsignieranforderung (CSR) für das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization an die Zertifizierungsstelle. Dies ist ein temporäres Zertifikat, das standardmäßig 24 Stunden lang gültig ist. Die Zertifizierungsstelle stellt dieses Zertifikat nicht automatisch aus. Die Ausstellung muss bei der Zertifizierungsstelle manuell von einem Administrator genehmigt werden. Wenn das Zertifikat für den FAS-Server ausgestellt wurde, verwendet der Verbundauthentifizierungsdienst das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization, um automatisch das Zertifikat Citrix_RegistrationAuthority (zwei Jahre gültig) abzurufen. Der FAS-Server löscht das Zertifikat und den Schlüssel für Citrix_RegistrationAuthority_ManualAuthorization, sobald er das Zertifikat Citrix_RegistrationAuthority erhält.

Der private Schlüssel des RA-Zertifikates ist besonders vertraulich, da die RA-Zertifikatrichtlinie dem Besitzer des privaten Schlüssels das Ausstellen von Zertifikatanforderungen für die in der Vorlage konfigurierten Benutzer erlaubt. Wer also diesen Schlüssel hat, kann als einer der konfigurierten Benutzer eine Verbindung mit der Umgebung herstellen.

Mit einer der folgenden Optionen können Sie die Konfiguration des FAS-Servers so festlegen, dass private Schlüssel den Sicherheitsanforderungen Ihrer Organisation entsprechend geschützt sind:

- Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von RA-Zertifikaten und von Benutzerzertifikaten.
- Schlüsselspeicheranbieter der Microsoft-Plattform mit einem Trusted Platform Module (TPM)-Chip für den privaten Schlüssel des RA-Zertifikats und Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von Benutzern.
- Ein Hardwaresicherheitsmodul (HSM) mit dem Kryptografiedienst eines Anbieters oder ein Schlüsselspeicheranbieter mit dem HSM-Gerät für das RA-Zertifikat und die privaten Schlüssel der Benutzerzertifikate.

## Konfigurationseinstellungen für private Schlüssel

Konfigurieren Sie den Verbundauthentifizierungsdienst, sodass er eine der drei Optionen verwendet. Bearbeiten Sie die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Datei Citrix.Authentication.FederatedAuthenticationService.exe.config mit einem Text-Editor. Der Standardspeicherort der Datei ist unter Programme\Citrix\Federated Authentication Service auf dem FAS-Server.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Der Verbundauthentifizierungsdienst liest die Konfigurationsdatei nur, wenn der Dienst gestartet wird. Wenn Sie Werte ändern, muss der FAS neu gestartet werden, damit die neuen Einstellungen wirksam werden.

Legen Sie die relevanten Werte in der Datei Citrix.Authentication.FederatedAuthenticationService.exe.config wie folgt fest:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (Wechsel zwischen CAPI und CNG-APIs)

| Wert | Kommentar |
|---|---|
| true | Verwenden Sie CAPIs |
| false (Standardwert) | Verwenden Sie CNG-APIs |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (ProviderName = Name des zu verwendenden Anbieters)

| Wert | Kommentar |
|---|---|
| Microsoft Enhanced RSA und AES Cryptographic Provider | CAPI-Standardanbieter |
| Schlüsselspeicheranbieter für Microsoft-Software | CNG-Standardanbieter |
| | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Schlüsselspeicheranbieter der Microsoft-Plattform | TPM-Standardanbieter TPM wird nicht für Benutzerschlüssel empfohlen. Verwenden Sie TPM nur für RA-Schlüssel. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie die TPM- und Hypervisor-Hersteller, ob Virtualisierung unterstützt wird. |
| HSM_Vendor CSP/Schlüsselspeicheranbieter | Bereitstellung durch HSM-Hersteller. Der Wert unterscheidet sich je nach Hersteller. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller, ob Virtualisierung unterstützt wird. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (Nur bei CAPI erforderlich)

| Wert | Kommentar |
|---|---|
| 24 | Standard. Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Wenn der FAS einen Privatschlüsselvorgang ausführen muss, wird der hier angegebene Wert verwendet.) Steuert das Flag "exportable" von privaten Schlüsseln. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers, wenn die Hardware dies unterstützt.

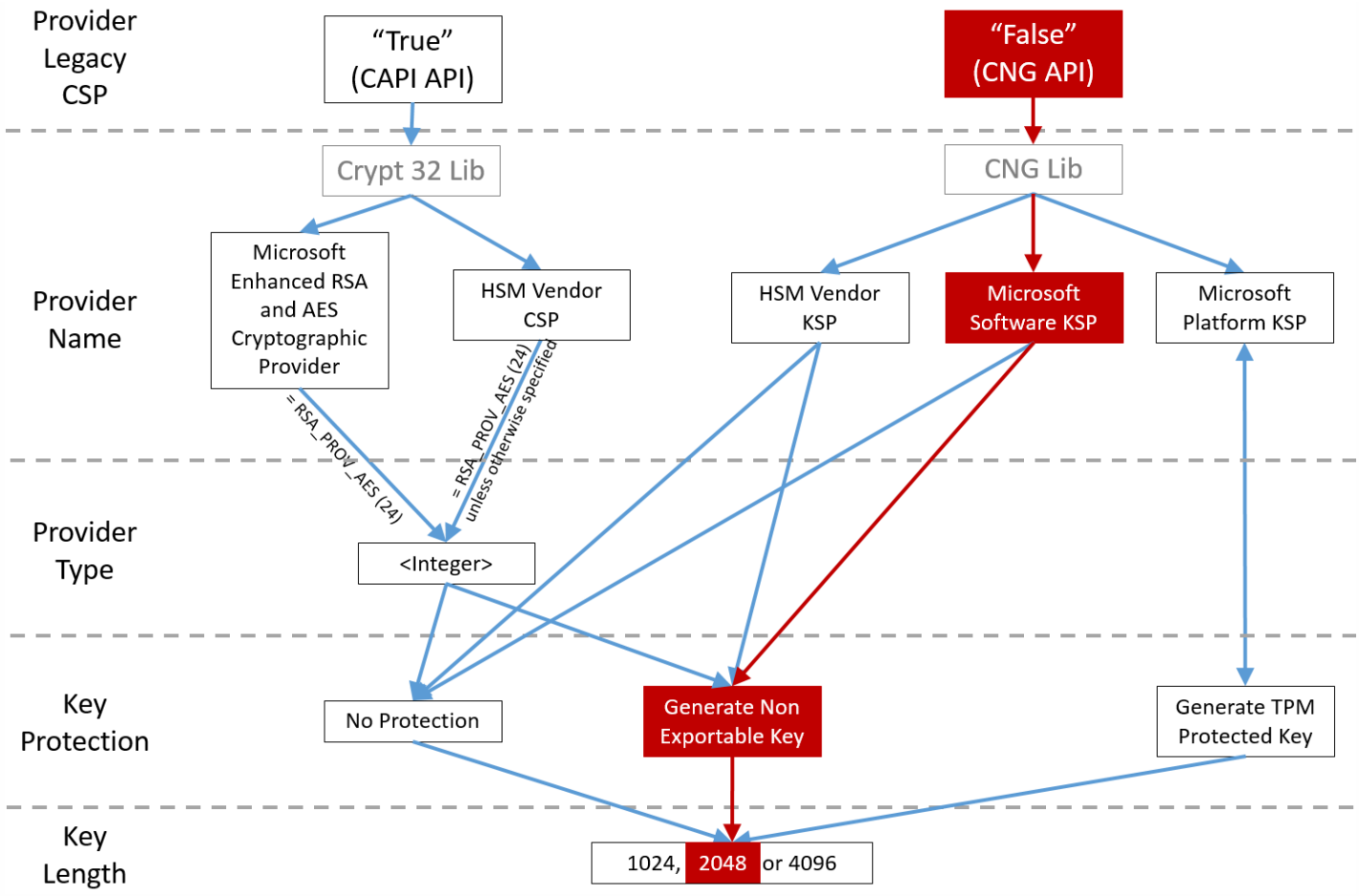
| Wert | Kommentar |
|---|---|
| NoProtection | Privater Schlüssel kann exportiert werden. |
| GenerateNonExportableKey | Standard. Privater Schlüssel kann nicht exportiert werden. |
| GenerateTPMProtectedKey | Privater Schlüssel wird mit dem TPM verwaltet. Der private Schlüssel wird von dem Anbieter gespeichert, den Sie in ProviderName angegeben haben (z. B. Schlüsselspeicheranbieter der Microsoft-Plattform) |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Geben Sie die Größe des privaten Schlüssels in Bit an.)

| Wert | Kommentar |
|---|---|
| 2048 | Standard. 1024 oder 4096 können auch verwendet werden. |

Die Einstellungen für die Konfigurationsdatei werden grafisch wie folgt dargestellt (Installationsstandards sind rot markiert):


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Beispiele für Konfigurationsszenarios

### Beispiel 1

Dieses Beispiel gilt für den privaten Schlüssel des RA-Zertifikats und die privaten Schlüssel der Benutzerzertifikate, die mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

Dies ist die Standardkonfiguration nach der Installation. Eine zusätzliche Konfiguration des privaten Schlüssels ist nicht erforderlich.

### Beispiel 2

Dieses Beispiel zeigt den privaten Schlüssel des RA-Zertifikats, der im FAS-Server auf der Hauptplatine im Hardware-TPM vom Schlüsselspeicheranbieter der Microsoft-Plattform gespeichert wurde, sowie die privaten Schlüssel der Benutzerzertifikate, die vom Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

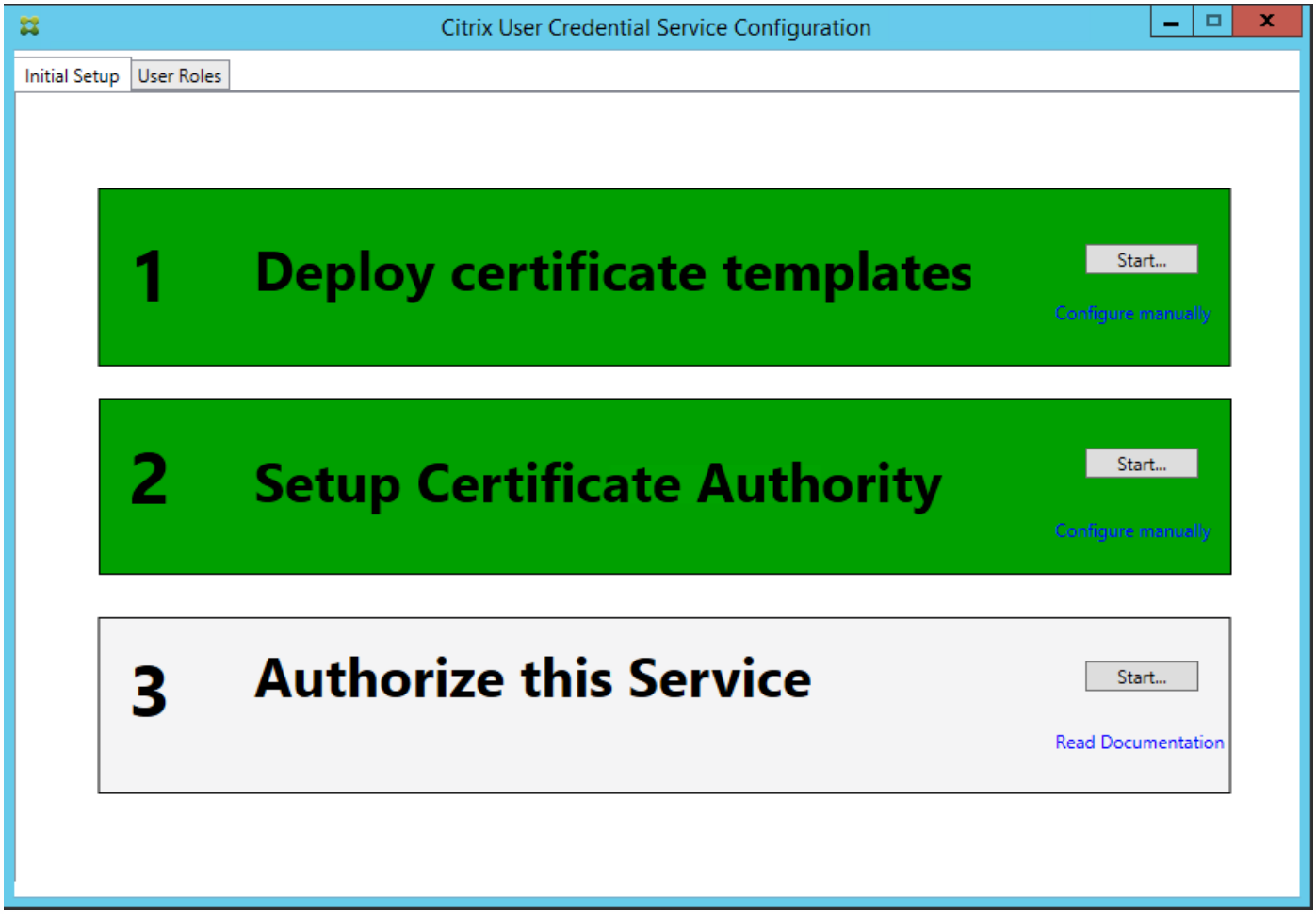
In diesem Szenario wird angenommen, dass das TPM auf der Hauptplatine des FAS-Servers im BIOS entsprechend der TPM-Herstellerdokumentation aktiviert und dann in Windows initialisiert wurde. Weitere Informationen finden Sie unter https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx.

## Verwenden von PowerShell (empfohlen)


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Das RA-Zertifikat kann offline mit PowerShell angefordert werden. Dies ist für Organisationen geeignet, wenn die Zertifizierungsstellen keine RA-Zertifikate über eine Online-Zertifikatsignieranforderung ausstellen dürfen. Eine Offline-Zertifikatsignieranforderung kann von einer Registrierungsstelle nicht über die FAS-Verwaltungskonsole ausgestellt werden.

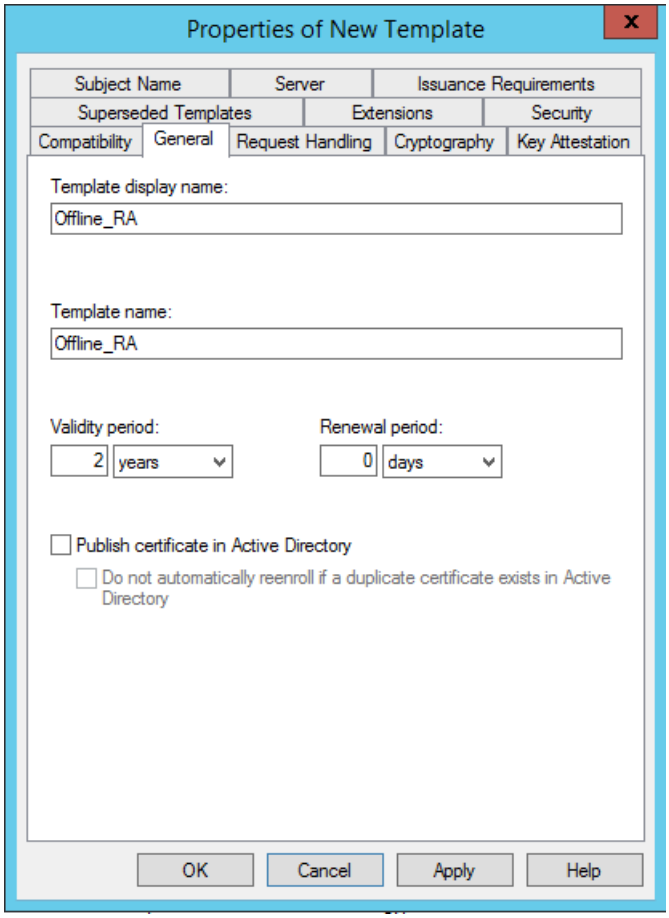
**Schritt 1:** Führen Sie während der Ersteinrichtung der FAS-Konfiguration mit der Verwaltungskonsole nur die ersten zwei Schritte aus: "Deploy certificate templates" und "Setup Certificate Authority".




**Schritt 2:** Fügen Sie auf dem Zertifizierungsstellenserver in der MMC das Zertifikatvorlagen-Snap-In hinzu. Klicken Sie mit der rechten Maustaste auf die Vorlage **Citrix_RegistrationAuthority_ManualAuthorization** und wählen Sie **Vorlage duplizieren**.

Wählen Sie die Registerkarte **Allgemein**. Ändern Sie den Namen und die Gültigkeitsdauer. In diesem Beispiel lautet der Name Offline_RA und die Gültigkeitsdauer ist 2 Jahre:


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Schritt 3:** Fügen Sie auf dem Zertifizierungsstellenserver in der MMC das Zertifizierungsstellen-Snap-In hinzu. Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**. Klicken Sie auf **Neu** und dann auf **Auszustellende Zertifikatvorlage**. Wählen Sie die Vorlage aus, die Sie soeben erstellt haben.

**Schritt 4:** Laden Sie die folgenden PowerShell-Cmdlets auf den FAS-Server:

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationServices.V1
```

**Schritt 5:** Erstellen Sie das RSA-Schlüsselpaar im TPM des FAS-Servers und erstellen Sie die Zertifikatsignieranforderung durch Eingabe des folgenden PowerShell-Cmdlets auf dem FAS-Server. **Hinweis:** Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Geben Sie eine Schlüssellänge an, die Ihre Hardware unterstützt.

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address
```

Beispiel:

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

Folgendes wird angezeigt:

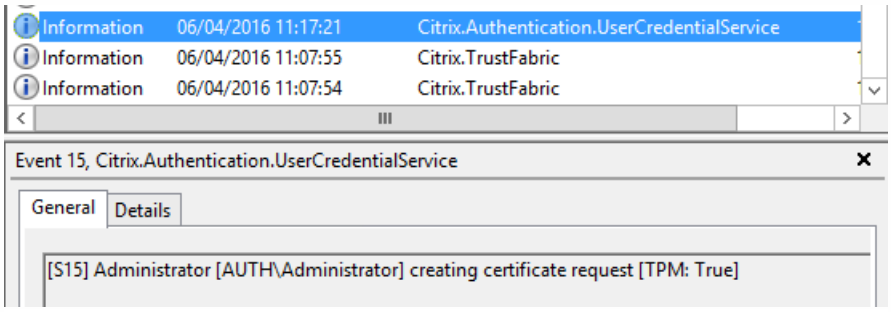

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Dy/WsPgPBgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH>
```

Hinweise:

- Die ID GUID (in diesem Beispiel "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") ist in einem der folgenden Schritte erforderlich.
- Betrachten Sie das PowerShell-Cmdlet als einmalige "Überschreibungsmethode" zum Generieren des privaten Schlüssels für das RA-Zertifikat.
- Wenn dieses Cmdlet ausgeführt wird, wird die zu verwendende Schlüssellänge anhand der Werte bestimmt, die beim Start des FAS-Diensts aus der Konfigurationsdatei gelesen wurden (der Standardwert ist 2048).
- Da -UseTPM in diesem manuellen, mit PowerShell initiierten Privatschlüsselvorgang für das RA-Zertifikat auf $true festgelegt ist, ignoriert das System Werte aus der Datei, die nicht mit den Einstellungen übereinstimmen, die zur Verwendung eines TPM erforderlich sind.
- Durch das Ausführen des Cmdlets ändern sich keine Einstellungen in der Konfigurationsdatei.
- Bei nachfolgenden automatischen, vom FAS initiierten Privatschlüsselvorgängen für Benutzerzertifikate werden die Werte verwendet, die beim Starten des FAS-Diensts aus der Datei gelesen wurden.
- Es ist auch möglich, den Wert KeyProtection in der Konfigurationsdatei auf GenerateTPMProtectedKey festzulegen, wenn der FAS-Server Benutzerzertifikate festlegt, damit durch das TPM geschützte private Schlüssel für Benutzerzertifikate generiert werden.

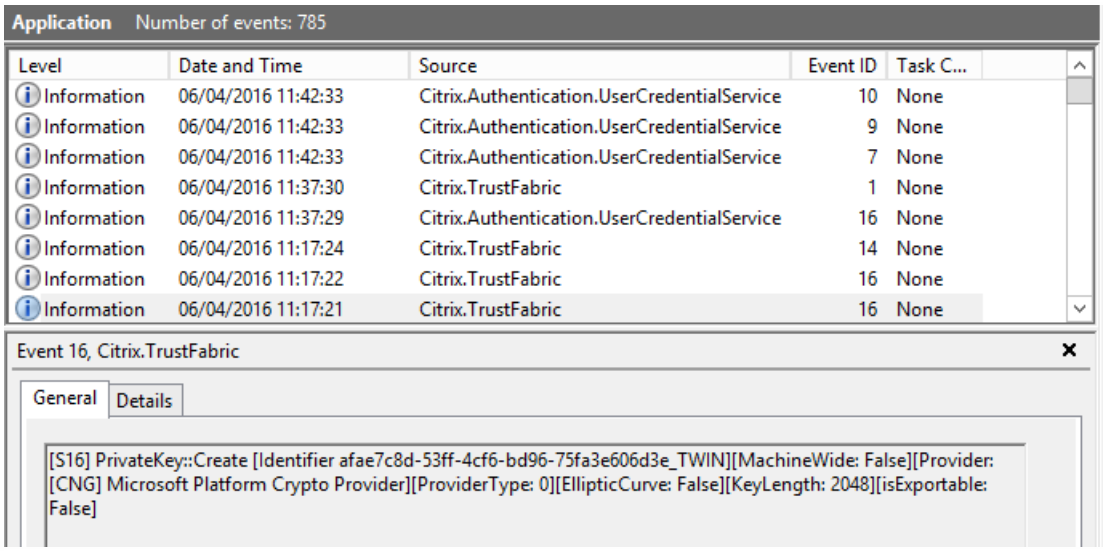
Um sicherzustellen, dass das TPM zum Generieren des Schlüsselpaars verwendet wurde, überprüfen Sie das Anwendungsprotokoll in der Windows-Ereignisanzeige auf dem FAS-Server auf die Zeit, zu der das Schlüsselpaar generiert wurde.




Folgendes sollte angezeigt werden: [TPM: True]

Gefolgt von:


© 1999-2017 Citrix Systems, Inc. All rights reserved.



Application Number of events: 785

| Level | Date and Time | Source | Event ID | Task C... |
|---|---|---|---|---|
| Information | 06/04/2016 11:42:33 | Citrix.Authentication.UserCredentialService | 10 | None |
| Information | 06/04/2016 11:42:33 | Citrix.Authentication.UserCredentialService | 9 | None |
| Information | 06/04/2016 11:42:33 | Citrix.Authentication.UserCredentialService | 7 | None |
| Information | 06/04/2016 11:37:30 | Citrix.TrustFabric | 1 | None |
| Information | 06/04/2016 11:37:29 | Citrix.Authentication.UserCredentialService | 16 | None |
| Information | 06/04/2016 11:17:24 | Citrix.TrustFabric | 14 | None |
| Information | 06/04/2016 11:17:22 | Citrix.TrustFabric | 16 | None |
| Information | 06/04/2016 11:17:21 | Citrix.TrustFabric | 16 | None |

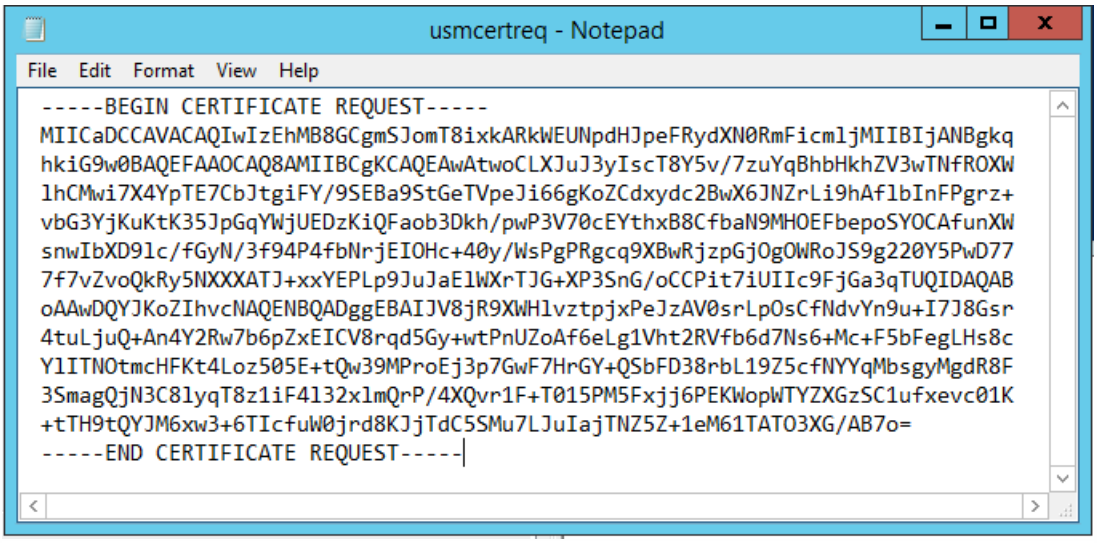
Event 16, Citrix.TrustFabric

General Details

[S16] PrivateKey::Create [Identifier afae7c8d-53ff-4cf6-bd96-75fa3e606d3e_TWIN][MachineWide: False][Provider: [CNG] Microsoft Platform Crypto Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]

Folgendes sollte angezeigt werden: "Provider: [CNG] Microsoft Platform Crypto Provider"

**Schritt 6:** Kopieren Sie den Abschnitt mit der Zertifikatanforderung in einen Texteditor und speichern Sie ihn als Textdatei auf einen Datenträger.



usmcertreq - Notepad

File Edit Format View Help


```
-----BEGIN CERTIFICATE REQUEST-----
MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V70cEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+40y/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g220Y5PwD77
7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaElWXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAV0srLpOsCfNdvYn9u+I7J8Gsr
4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
YlITNOtmcHFKt4Loz505E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+T015PM5Fxjj6PEKWopWTYZXGzSC1ufxevc01K
+tTH9tQYJM6xw3+6TIcfuW0jrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
-----END CERTIFICATE REQUEST-----
```


**Schritt 7:** Senden Sie die Zertifikatsignieranforderung an die Zertifizierungsstelle, indem Sie auf dem FAS-Server Folgendes in PowerShell eingeben:

```
certreq -submit -attrib "certificatetemplate:"
```

Beispiel:

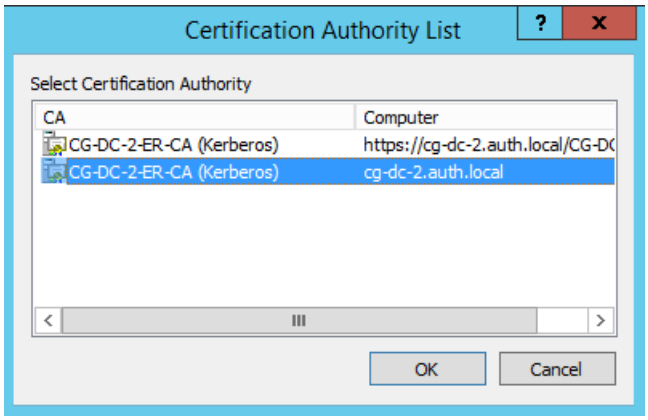
```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

Folgendes wird angezeigt:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-4D21-A4FD-2E29502177C2}
  ldap:
```

An dieser Stelle wird u. U. ein Fenster mit einer Liste der Zertifizierungsstellen angezeigt. Für die Zertifizierungsstelle in diesem Beispiel sind http- (oben) und DCOM-Registrierung (unten) aktiviert. Wählen Sie ggf. die DCOM-Option:



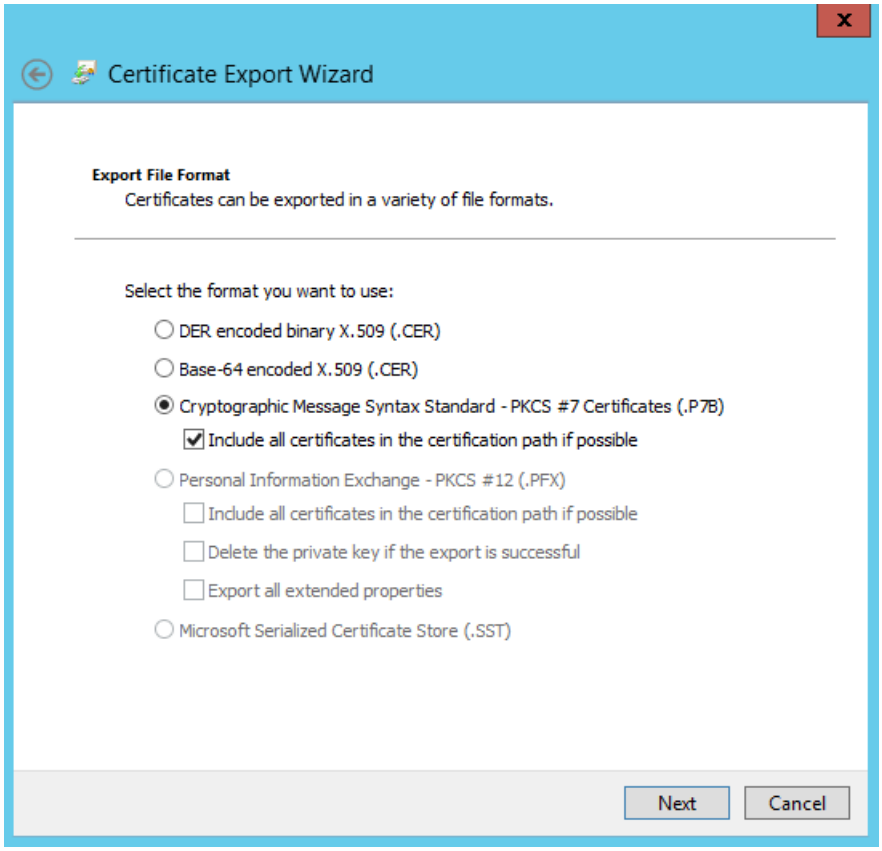

Nachdem die Zertifizierungsstelle angegeben wurde, zeigt PowerShell die RequestID an:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

**Schritt 8:** Klicken Sie auf dem Zertifizierungsstellenserver in der MMC im Zertifizierungsstellen-Snap-In auf **Ausstehende Anforderungen**. Suchen Sie die Anforderungs-ID (RequestID). Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

**Schritt 9:** Wählen Sie den Knoten **Ausgestellte Zertifikate**. Suchen Sie das Zertifikat, das soeben ausgestellt wurde (die Anforderungs-ID muss übereinstimmen). Doppelklicken Sie auf das Zertifikat, um es zu öffnen. Klicken Sie auf die Registerkarte **Details**. Klicken Sie auf **In Datei kopieren**. Der Zertifikatexportassistent wird gestartet. Klicken Sie auf **Weiter**. Wählen Sie die folgenden Optionen für das Dateiformat:


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Das Format muss wie folgt sein: **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)** und **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** muss aktiviert sein.

**Schritt 10:** Kopieren Sie die exportierte Zertifikatdatei auf den FAS-Server.

**Schritt 11:** Importieren Sie das RA-Zertifikat in die Registrierung des FAS-Servers, indem Sie das folgende PowerShell-Cmdlet auf dem FAS-Server eingeben:

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

Beispiel:

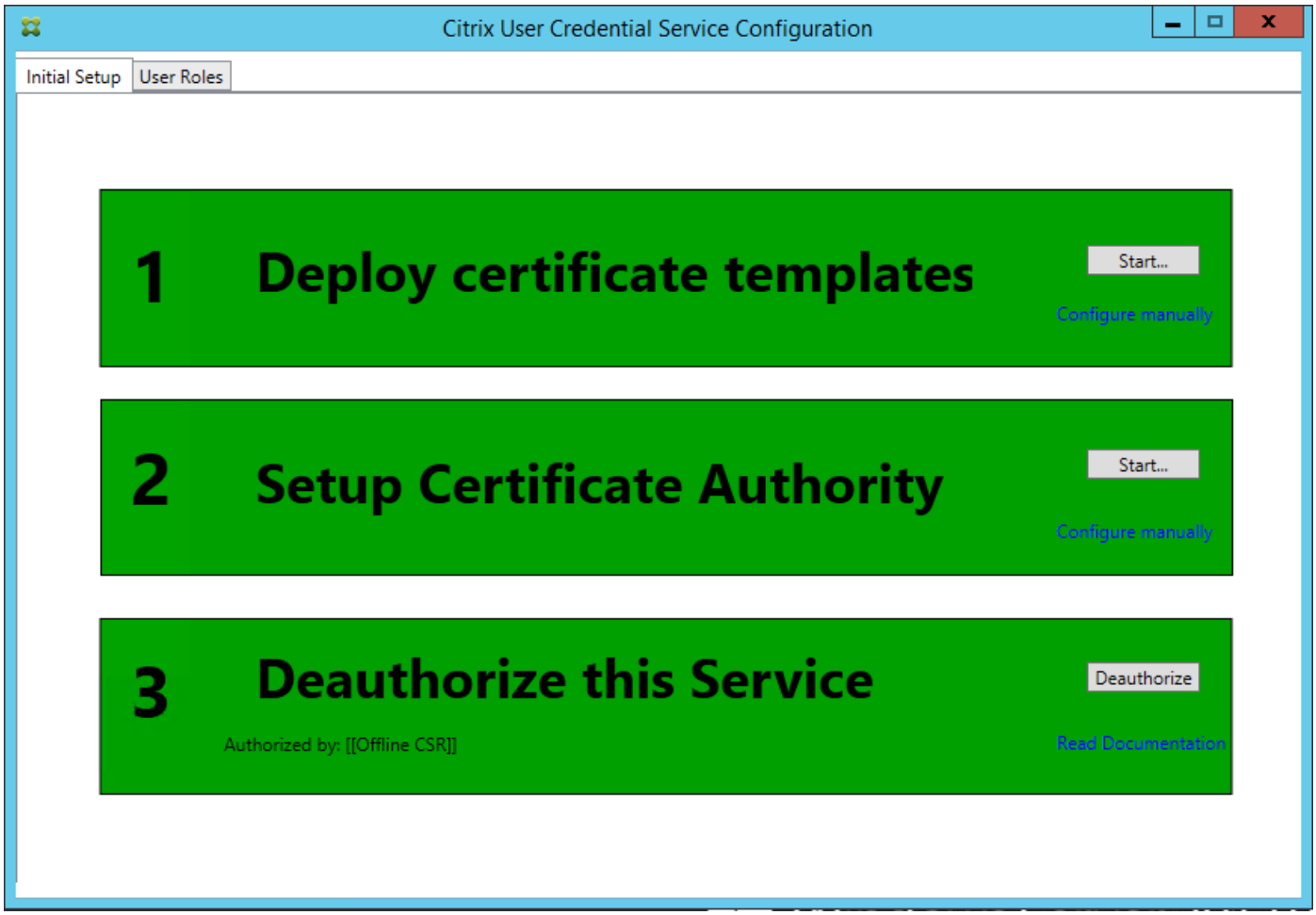
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

Folgendes wird angezeigt:

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec311020fc
CertificateRequest  :
Status              : Ok
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Schritt 12:** Schließen Sie die FAS-Verwaltungskonsole und starten Sie sie neu.




Der Schritt "Authorize this Service" ist nun grün und der Text lautet nun "Deauthorize this Service" und darunter "Authorized by: Offline CSR".

**Schritt 13:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **User Roles** und bearbeiten Sie die Einstellungen entsprechend den Anleitungen im FAS-Hauptartikel.

Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

## Verwenden der FAS-Verwaltungskonsole

Die FAS-Verwaltungskonsole kann keine Offline-Zertifikatsignieranforderung ausstellen, daher wird die Verwendung nicht empfohlen, es sei denn, Ihre Organisation erlaubt Online-Zertifikatsignieranforderungen für RA-Zertifikate.

Führen Sie bei der Ersteinrichtung des Verbundauthentifizierungsdiensts die folgenden Schritte aus, und zwar nach der Bereitstellung der Zertifikatvorlagen und der Einrichtung der Zertifizierungsstelle, aber bevor Sie den Dienst autorisieren (Schritt 3 in der Konfigurationsreihenfolge):

**Schritt 1:** Bearbeiten Sie die Konfigurationsdatei, indem Sie die folgende Zeile folgendermaßen ändern:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Daraufhin sollte die Datei wie folgt aussehen:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Geben Sie eine Schlüssellänge an, die Ihre Hardware unterstützt.

**Schritt 2:** Autorisieren Sie den Dienst.

**Schritt 3:** Stellen Sie manuell die ausstehende Zertifikatanforderung des Zertifizierungsstellenservers aus. Nachdem Sie das RA-Zertifikat erhalten haben, wird Schritt 3 der Einrichtungsreihenfolge in der Verwaltungskonsole grün angezeigt. Der private Schlüssel für das RA-Zertifikat wurde nun im TPM generiert. Das Zertifikat gilt standardmäßig 2 Jahre.

**Schritt 4:** Ändern Sie die Konfigurationsdatei nun wieder wie folgt:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

Hinweis: Obwohl der Verbundauthentifizierungsdienst Benutzerzertifikate mit TPM-geschützten Schlüsseln generieren kann, ist die TPM-Hardware möglicherweise zu langsam für große Bereitstellungen.

**Schritt 5:** Starten Sie den Citrix Verbundauthentifizierungsdienst neu. Dadurch wird der Dienst gezwungen, die Konfigurationsdatei erneut zu lesen und die geänderten Werte werden wirksam. Die nachfolgenden automatischen Privatschlüsselvorgänge wirken sich auf Benutzerzertifikatschlüssel aus. Bei diesen Vorgängen werden die privaten Schlüssel nicht im TPM, sondern mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert.

**Schritt 6:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte "User Roles" und bearbeiten Sie die Einstellungen wie im FAS-Hauptartikel beschrieben.

Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

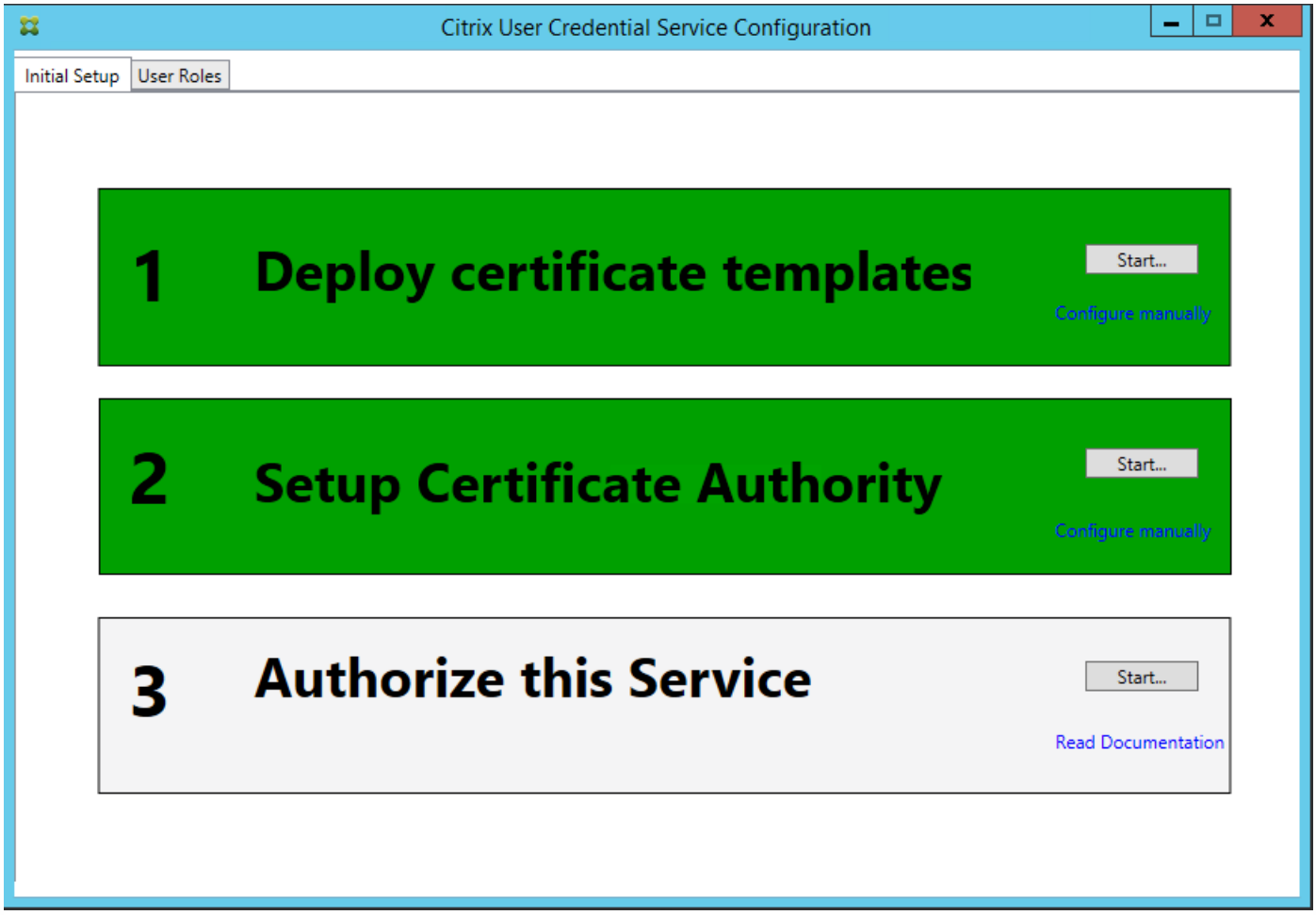

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Beispiel 3

Dieses Beispiel gilt für einen privaten Schlüssel des RA-Zertifikats und die privaten Schlüssel der Benutzerzertifikate, die in einem HSM gespeichert wurden. In diesem Beispiel wird ein konfiguriertes HSM vorausgesetzt. Das HSM hat einen Anbieternamen, z. B. "HSM_Vendor's Key Storage Provider".

Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller nach Hypervisor-Unterstützung.

**Schritt 1:** Führen Sie während der Ersteinrichtung der FAS-Konfiguration mit der Verwaltungskonsole nur die ersten zwei Schritte aus: "Deploy certificate templates" und "Setup Certificate Authority".




**Schritt 2:** Aus der Dokumentation Ihres HSM erfahren Sie, welchen Wert der ProviderName Ihres HSM haben sollte. Wenn das HSM CAPI verwendet, wird der Anbieter in der Dokumentation möglicherweise als Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) bezeichnet. Wenn das HSM CNG verwendet, wird der Anbieter möglicherweise als Schlüsselspeicheranbieter (Key Storage Provider, KSP) bezeichnet.

**Schritt 3:** Bearbeiten Sie die Konfigurationsdatei wie folgt:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Daraufhin sollte die Datei wie folgt aussehen:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

In diesem Szenario wird angenommen, dass Ihr HSM CNG verwendet, daher ist der Wert von ProviderLegacyCsp "false". Wenn das HSM CAPI verwendet, sollte der Wert für ProviderLegacyCsp auf "true" festgelegt sein. Sie erfahren aus der Dokumentation des HSM-Herstellers, ob das HSM CAPI oder CNG verwendet. Außerdem erfahren Sie aus der Dokumentation, welche Schlüssellängen für die Generierung eines asymmetrischen RSA-Schlüssels das HSM unterstützt. In diesem Beispiel ist die Schlüssellänge auf den Standardwert von 2048 Bit festgelegt. Stellen Sie sicher, dass die von Ihnen festgelegte Schlüssellänge von der Hardware unterstützt wird.

**Schritt 4:** Starten Sie den Citrix Verbundauthentifizierungsdienst neu, damit die Werte in der Konfigurationsdatei gelesen werden.

**Schritt 5:** Generieren Sie das RSA-Schlüsselpaar im HSM und erstellen Sie die Zertifikatsignieranforderung, indem Sie auf der Registerkarte "Initial Setup" der FAS-Verwaltungskonsole auf **Authorize** klicken.

**Schritt 6:** Stellen Sie sicher, dass das Schlüsselpaar im HSM erstellt wurde, indem Sie die Anwendungseinträge im Windows-Ereignisprotokoll überprüfen:

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

Folgendes sollte angezeigt werden: [Provider: [CNG] HSM_Vendor's Key Storage Provider]

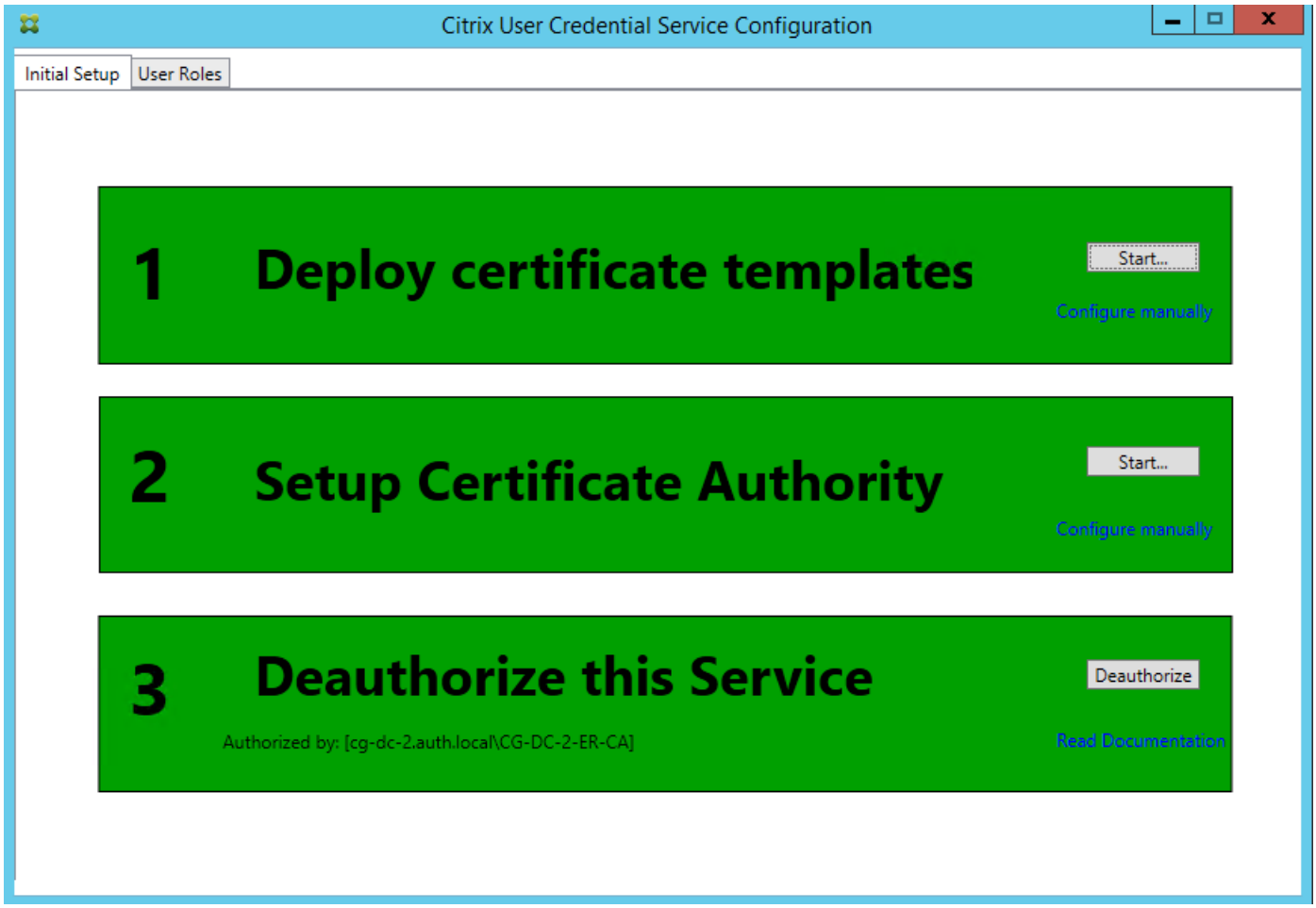
**Schritt 7:** Wählen Sie auf dem Zertifizierungsstellenserver in der Zertifizierungsstellen-MMC den Knoten **Ausstehende Anforderungen**:

| Request ID | Binary Request | Request Status Code | Request Disposition Message | Request Submission Date | Requester Name | Request Country/Region |
|---|---|---|---|---|---|---|
| 107 | -----BEGIN NE... | The operation compl... | Taken Under Submission | 07/04/2016 14:04 | AUTH\UCSHSM$ | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

Der Schritt "Authorize this Service" ist nun grün und der Text lautet nun "Deauthorize this Service" und darunter "Authorized by: []".




**Schritt 8:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **User Roles** und bearbeiten Sie die Einstellungen wie im FAS-Hauptartikel beschrieben.

Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

# FAS-Zertifikatspeicher

Der Verbundauthentifizierungsdienst verwendet nicht den Microsoft Zertifikatspeicher auf dem FAS-Server, um Zertifikate zu speichern. Stattdessen wird die Registrierung verwendet.

Hinweis: Wenn Sie ein HSM zum Speichern der privaten Schlüssel verwenden, werden die HSM-Container durch GUIDs identifiziert. Die GUID für den privaten Schlüssel im HSM stimmt mit der GUID für das entsprechende Zertifikat in der Registrierung überein.

Um die GUID für das RA-Zertifikat zu ermitteln, geben Sie die folgenden PowerShell-Cmdlets auf dem FAS-Server ein:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address

Beispiel:

Get-FasAuthorizationCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest  :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEg0xlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      GlO/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

Geben Sie zum Abrufen einer Liste mit Benutzerzertifikaten Folgendes ein:

Get-FasUserCertificate –address

Beispiel:

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

# Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sicherheits- und Netzwerkkonfiguration für den Verbundauthentifizierungsdienst

Jul 13, 2016

Der Citrix Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eng in Microsoft Active Directory und die Microsoft-Zertifizierungsstelle integriert. Es ist wichtig, das System richtig zu verwalten und zu schützen. Hierfür muss, wie bei Domänencontrollern oder anderen wichtige Infrastrukturkomponenten auch, eine geeignete Sicherheitsrichtlinie entwickelt werden.

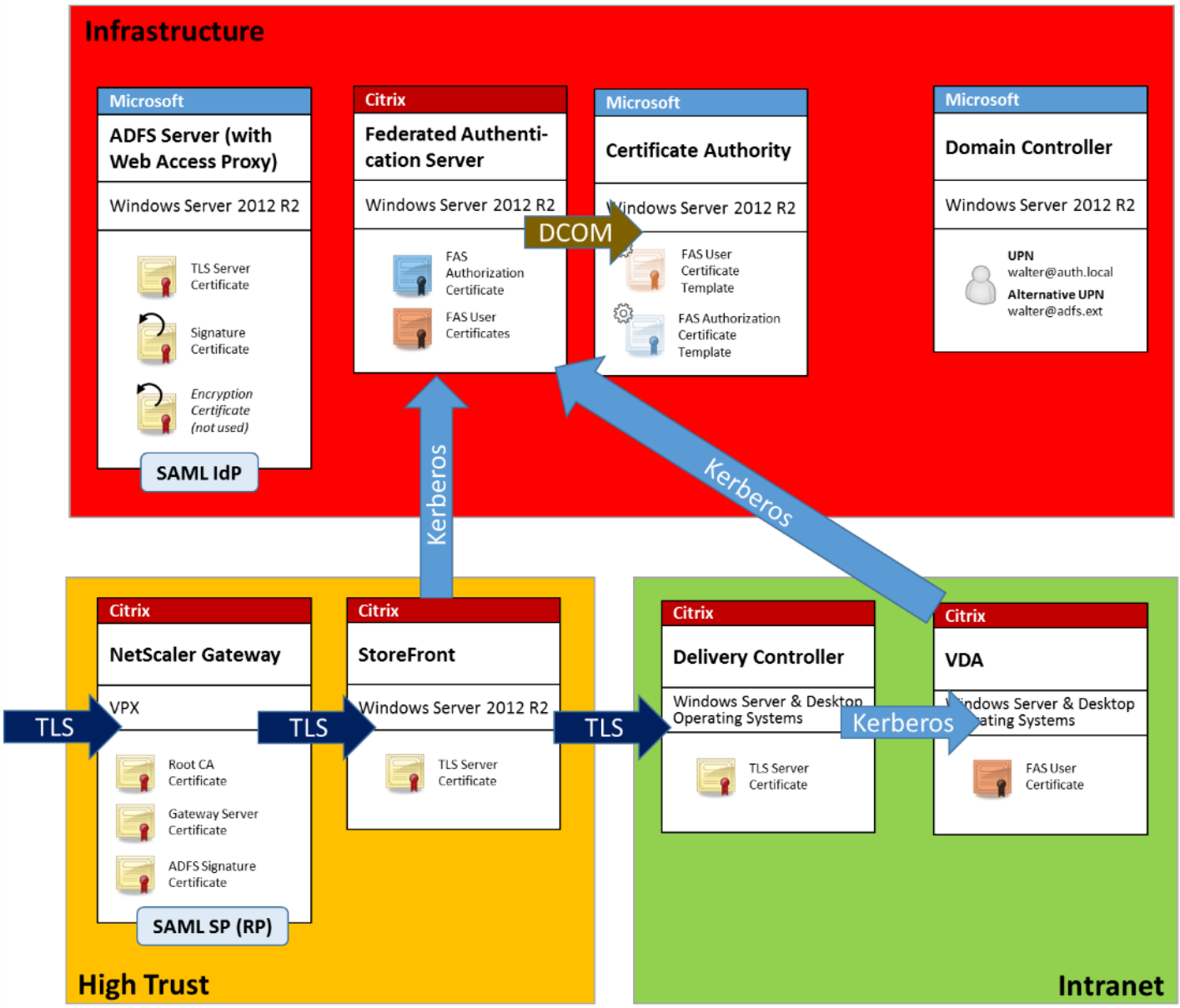
Dieses Dokument enthält eine Übersicht über die Sicherheitsfragen, die Sie bei der FAS-Bereitstellung berücksichtigen sollten. Außerdem finden Sie hier eine Übersicht über die Features, die Ihnen beim Schutz der Infrastruktur helfen können.

## Netzwerkarchitektur

Die folgende Abbildung zeigt die wichtigsten Komponenten und Sicherheitsgrenzen einer FAS-Bereitstellung.

Der FAS-Server gilt zusammen mit der Zertifizierungsstelle und dem Domänencontroller als Teil der sicherheitskritischen Infrastruktur. In einer Verbundumgebung haben NetScaler und StoreFront eine Vertrauensstellung zur Durchführung der Benutzerauthentifizierung. Andere XenApp- und XenDesktop-Komponenten werden von einer FAS-Implementierung nicht betroffen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Firewall und Netzwerksicherheit

Die Kommunikation zwischen NetScaler, StoreFront und den Delivery Controller-Komponenten muss durch TLS über Port 443 geschützt werden. Der StoreFront-Server führt nur ausgehende Verbindungen durch und NetScaler Gateway darf nur Verbindungen über das Internet mit HTTPS-Port 443 akzeptieren.

Der StoreFront-Server kontaktiert den FAS-Server über Port 80 unter Verwendung von beidseitig authentifiziertem Kerberos. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computerkontoidentität des StoreFront-Servers verwendet. Dadurch wird ein Anmeldehandle für die einmalige Verwendung erstellt, das der Citrix Virtual Delivery Agent (VDA) zur Anmeldung des Benutzers benötigt.

Wenn eine HDX-Sitzung mit dem VDA verbunden wird, kontaktiert der VDA außerdem den FAS-Server über Port 80. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computeridentität des


© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAs verwendet. Außerdem muss der VDA das Anmeldeinformations-Handle übergeben, um auf Zertifikat und privaten Schlüssel zugreifen zu können.

Die Microsoft-Zertifizierungsstelle akzeptiert Kommunikation mit einem Kerberos-authentifizierten DCOM, das zur Verwendung eines festen TCP-Ports konfiguriert werden kann. Die Zertifizierungsstelle erfordert außerdem, dass der FAS-Server ein durch ein vertrauenswürdiges Enrollment Agent-Zertifikat signiertes CMC-Paket übergibt.

| Server | Firewallports |
|---|---|
| Verbundauthentifizierungsdienst | (eingehend) Kerberos über HTTP von StoreFront und VDAs<br>(ausgehend) DCOM an Microsoft-Zertifizierungsstelle |
| NetScaler | (eingehend) HTTPS von Clientmaschinen<br>(ein-/ausgehend) HTTPS an/von StoreFront-Server<br>(ausgehend) HDX an VDA |
| StoreFront | (eingehend) HTTPS von NetScaler<br>(ausgehend) HTTPS an Delivery Controller<br>(ausgehend) Kerberos HTTP an FAS |
| Delivery Controller | (eingehend) HTTPS von StoreFront-Server<br>(ein/ausgehend) Kerberos über HTTP von VDAs |
| VDA | (ein/ausgehend) Kerberos über HTTP von Delivery Controller<br>(eingehend) HDX von NetScaler Gateway<br>(ausgehend) Kerberos HTTP an FAS |
| Microsoft CA | (eingehend) DCOM und signiert von FAS |

# Verwaltungsaufgaben

Die Verwaltung der Umgebung lässt sich in folgende Zuständigkeiten aufgliedern:

| Name | Aufgaben |
|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Unternehmensadministrator | Installation und Schutz von Zertifikatvorlagen in der Gesamtstruktur |
| Domänenadministrator | Konfiguration der Gruppenrichtlinieneinstellungen |
| Zertifizierungsstellenadministrator | Konfigurieren der Zertifizierungsstelle |
| FAS-Administrator | Installieren und konfigurieren des FAS-Servers |
| StoreFront-/NetScaler-Administrator | Konfigurieren der Benutzerauthentifizierung |
| XenDesktop-Administrator | Konfigurieren von VDAs und Controllern |

Jeder Administrator ist für verschiedene Aspekte des allgemeinen Sicherheitsmodells zuständig, sodass ein Defense-in-Depth-Schutz des Systems möglich ist.

# Gruppenrichtlinieneinstellungen

Vertrauenswürdige FAS-Maschinen werden anhand einer über die Gruppenrichtlinie konfigurierten Nachschlagetabelle mit Indexnummer -> FQDN identifiziert. Beim Herstellen einer Verbindung mit dem FAS-Server prüfen Clients dessen HOST\ Kerberos-Identität. Alle Server, die auf den FAS-Server zugreifen, müssen die gleiche FQDN-Konfiguration für denselben Index haben, ansonsten stellen StoreFront und VDAs möglicherweise eine Verbindung mit verschiedenen FAS-Servern her.

Zur Vermeidung von Konfigurationsfehlern empfiehlt Citrix die Anwendung einer einzelnen Richtlinie auf alle Maschinen in der Umgebung. Vorsicht beim Bearbeiten der Liste der FAS-Server, insbesondere wenn Sie Einträge entfernen oder umsortieren.

Die Steuerung dieses Gruppenrichtlinienobjekts sollte auf FAS-Administratoren (und/oder Domänenadministratoren) beschränkt werden, die FAS-Server installieren und außer Betrieb nehmen. Die Wiederverwendung von Maschinen-FQDNs kurz nach der Außerbetriebnahme eines FAS-Servers ist zu vermeiden.

# Zertifikatvorlagen

Zertifikatvorlagen werden gesamtstrukturübergreifend vom Administrator installiert. Es gibt vier wichtige Sicherheitsüberlegungen.

**Installation von Registrierungsstellenvorlagen**

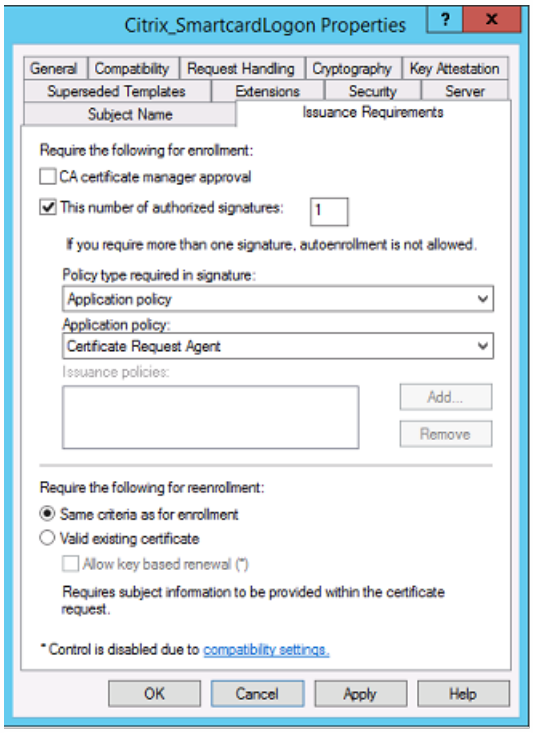
Das FAS-Installationsprogramm bietet zwei Arten von Zertifikatvorlagen: Registrierungsstellenzertifikate und die Vorlage für die Smartcard-Anmeldung.

Bei der Ausführung wird nur die die Vorlage für die Smartcard-Anmeldung benötigt. Die Registrierungsstellenzertifikate brauchen also entweder nicht installiert werden (d. h. sie müssen manuell mit über eine eigene Offline-ZS ausgestellt werden) oder sie können nach der Autorisierung des FAS-Servers deaktiviert werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Anwendungsrichtlinien-OID

Registrierungsstellenzertifikate werden durch eine Zertifikatanforderungs-Agent-OID in den Erweiterungen der erweiterten Schlüsselverwendung identifiziert. Wenn die Möglichkeit besteht, dass die OID von einem anderen System verwendet wird, kann sie in eine komplett benutzerdefinierte OID geändert werden.

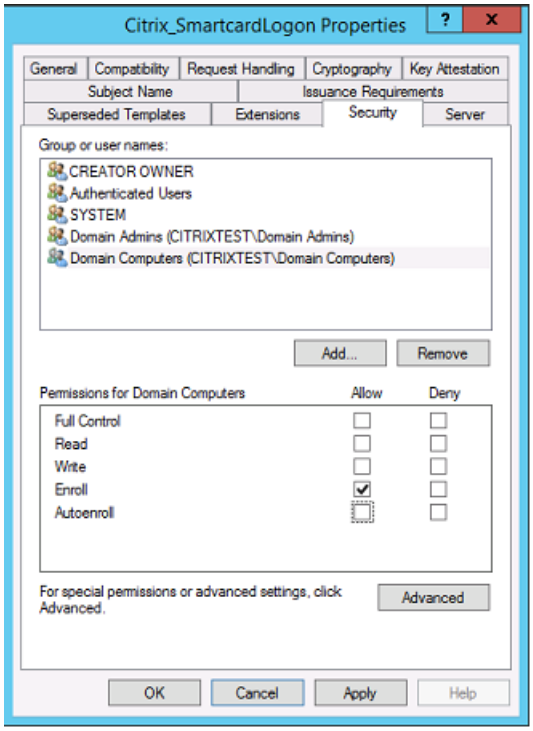



### Zugriffssteuerungsliste (ACL)

Jede Vorlage hat eine ACL, die festlegt, welche Benutzer und Computer Zertifikate ausstellen können.

Citrix empfiehlt, die ACL so zu konfigurieren, dass nur die Computerkonten der FAS-Server Zertifikate anfordern können. Dies kann über Netzwerkfirewallrichtlinien weiter eingeschränkt werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Einschränkungen bezüglich Antragstellernamen, Erweiterungen und Pfad**

Standardantragstellername und Erweiterungen können mit den standardmäßigen RFC 5280-Features konfiguriert werden, um festzulegen, für welche Zwecke ausgestellte Zertifikate verwendet werden können. Damit bietet sich eine einfache Möglichkeit der Steuerung, wofür die über die Public Key-Infrastruktur (PKI) ausgestellten Zertifikate verwendet werden können.

# ZS-Verwaltung

Der ZS-Administrator ist für die Konfiguration des ZS-Servers und des von diesem für das Ausstellerzertifikat verwendeten privaten Schlüssels verantwortlich.

**Veröffentlichen von Vorlagen**

Damit eine Zertifizierungsstelle Zertifikate basierend auf einer vom Unternehmensadministrator bereitgestellten Vorlage ausstellen kann, muss der ZS-Administrator die Vorlage veröffentlichen.

Eine einfache Sicherheitsmaßnahme besteht darin, die Registrierungsstellenzertifikate nur zu veröffentlichen, wenn die FAS-Server installiert werden, oder ein Ausstellungsverfahren vorzuschreiben, das komplett offline ist. In beiden Fällen darf nur der ZS-Administrator Registrierungsstellenzertifikate autorisieren und er muss eine Richtlinie für die Autorisierung von FAS-Servern haben.

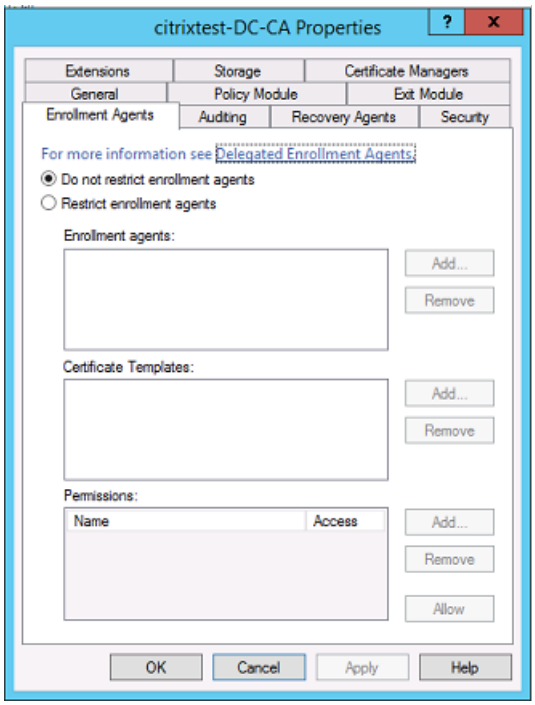
**Firewalleinstellungen**

Im Allgemeinen kann der ZS-Administrator auch die Firewalleinstellungen der Zertifizierungsstelle festlegen und somit eingehende Verbindungen steuern. Der ZS-Administrator kann DCOM TCP- und Firewallregeln so konfigurieren, dass nur FAS-Server Zertifikate anfordern können.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Eingeschränkte Registrierung

Standardmäßig kann jeder Eigentümer eines Registrierungsstellenzertifikats beliebigen Benutzern ein Zertifikat auf der Basis einer Zertifikatvorlage, die Zugriff ermöglicht, ausstellen. Dies sollte auf eine Gruppe von Benutzern ohne Privilegien über die ZS-Eigenschaft "Registrierungs-Agents einschränken" eingeschränkt werden.




### Richtlinienmodule und Überwachung

In komplexeren Bereitstellungen können benutzerdefinierte Sicherheitsmodule verwendet werden, um die Zertifikatausstellung zu verfolgen und zu unterbinden.

# FAS-Verwaltung

Der FAS hat mehrere Sicherheitsfeatures.

### Einschränken von StoreFront, Benutzern und VDAs über eine Zugriffssteuerungsliste

Im Zentrum des FAS-Sicherheitsmodells liegt die Steuerung des Zugriffs auf Funktionen durch Kerberos-Konten:

| Zugriffsvektor | Beschreibung |
|---|---|
| StoreFront (IdP) | Diese Kerberos-Konten können deklarieren, dass ein Benutzer korrekt authentifiziert wurde. Bei Gefährdung eines dieser Konten können Zertifikate erstellt und für durch die FAS-Konfiguration zugelassene Benutzer verwendet werden. |
| VDAs (vertrauende Seite) | Dies sind die Maschinen, die auf Zertifikate und private Schlüssel zugreifen dürfen. Zusätzlich ist ein vom IdP abgerufenes Anmelde-Handle erforderlich, sodass ein |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | gefährdetes VDA-Konto in dieser Gruppe nur geringe Möglichkeiten für einen Angriff auf das System hat. |
| Benutzer | Hierdurch wird gesteuert, welche Benutzer vom IdP bestätigt werden können. Es besteht eine Überschneidung mit den ZS-Optionen "Registrierungs-Agents einschränken".<br><br>Im Allgemeinen sollten nur nicht-privilegierte Benutzerkonten in diese Liste aufgenommen werden. Dies verhindert, dass ein gefährdetes StoreFront-Konto Privilegien auf eine höhere Verwaltungsebene übertragen kann. Vor allem Domänenadministratorkonten dürfen keine Berechtigung durch diese ACL erhalten. |

**Konfigurieren von Regeln**

Regeln sind nützlich, wenn mehrere eigenständige XenApp- oder XenDesktop-Bereitstellungen die gleiche FAS-Serverinfrastruktur verwenden. Jede Regel hat eigene Konfigurationsoptionen, wobei insbesondere separate Zugriffssteuerungslisten konfiguriert werden können.

**Konfigurieren von Zertifizierungsstellen und Vorlagen**

Für verschiedene Zugriffsrechte können verschiedene Zertifikatvorlagen und Zertifizierungsstellen konfiguriert werden. In komplexen Konfigurationen werden ggf. abhängig von der Umgebung weniger oder leistungsfähigere Zertifikate verwendet. Beispiel: Als extern identifizierte Benutzer können ein Zertifikat mit weniger Berechtigungen als interne Benutzer haben.

**Sitzungsinterne und Authentifizierungszertifikate**

Der FAS-Administrator kann festlegen, ob das für die Authentifizierung verwendete Zertifikat in der Sitzung eines Benutzers verwendet werden kann. Damit kann beispielsweise festgelegt werden, dass nur Signaturzertifikate sitzungsintern zur Verfügung stehen und die leistungsfähigeren Anmeldezertifikate nur bei der Anmeldung.

**Schutz privater Schlüssel und Schlüssellänge**

Der FAS-Administrator kann den FAS so konfigurieren, dass private Schlüssel in einem Hardwaresicherheitsmodul (HSM) oder einem Trusted Platform Module (TPM) gespeichert werden. Citrix empfiehlt, zumindest den privaten Schlüssel des Registrierungsstellenzertifikats durch Speicherung in einem TPM zu schützen. Diese Option kann im Offline-Verfahren für die Zertifikatanforderung gewählt werden.

Auch die privaten Schlüssel für Benutzerzertifikate können in einem TPM oder HSM gespeichert werden. Alle Schlüssel müssen als nicht exportierbar generiert werden und eine Länge von mindestens 2048 Bit haben.

**Ereignisprotokolle**

Der FAS-Server bietet detaillierte Konfigurations- und Laufzeit-Ereignisprotokolle, die für die Überwachung und Angriffserkennung verwendet werden können.

**Verwaltungszugriff und Verwaltungstools**

Der FAS umfasst Features und Tools zur Remoteverwaltung (unter gegenseitiger Kerberos-Authentifizierung). Mitglieder der lokalen Administratorgruppe haben Vollzugriff auf die FAS-Konfiguration. Diese Liste muss sorgfältig gepflegt werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# XenApp-, XenDesktop- und VDA-Administratoren

Generell ändert die Verwendung des FAS nichts am Sicherheitsmodell für Delivery Controller- und VDA-Administratoren, da das FAS-Anmeldeinformations-Handle direkt das Active Directory-Kennwort ersetzt. Controller- und VDA-Administratorgruppen dürfen nur vertrauenswürdige Benutzer enthalten. Es müssen Überwachungs- und Ereignisprotokolle geführt werden.

# Allgemeine Windows-Serversicherheit

Für alle Server müssen sämtliche Patches installiert sein und Standardfirewall- und Antivirensoftware zur Verfügung stehen. Sicherheitskritische Infrastrukturserver müssen an einem sicheren physischen Standort sein, Optionen für Datenträgerverschlüsselung und die Wartung virtueller Maschinen müssen sorgfältig gewählt werden.

Überwachungs- und Ereignisprotokolle müssen sicher auf einem Remotecomputer gespeichert werden.

Der RDP-Zugriff muss auf autorisierte Administratoren beschränkt werden. Soweit möglich sollten Benutzerkonten eine Smartcard-Anmeldung erfordern. Dies gilt insbesondere für Zertifizierungsstellen- und Domänenadministratorkonten.

# Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Einführung zu den FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Problembehandlung von Windows-Anmeldeproblemen mit dem Verbundauthentifizierungsdienst

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


- Zertifikate und Public Key-Infrastruktur
- Zuordnung von UPN-Namen und Zertifikaten
- Steuern der Domänencontrollerauswahl für die Anmeldung
- Aktivieren von Kontoüberwachungsereignissen
- Zertifikatüberprüfungsprotokolle
- Kerberos-Protokolle
- Ereignisprotokollmeldungen
- Endbenutzerfehlermeldungen
- Verwandte Informationen


In diesem Artikel werden die Protokolle und Fehlermeldungen beschrieben, die in Windows verfügbar sind, wenn sich Benutzer mit Zertifikaten und/oder Smartcards anmelden. Die Protokolle enthalten Informationen, die bei der Problembehandlung von Authentifizierungsfehlern hilfreich sein können.

## Zertifikate und Public Key-Infrastruktur

Windows Active Directory unterhält mehrere Zertifikatspeicher, in denen Zertifikate für Benutzer verwaltet werden, die sich anmelden.

- **NTAuth-Zertifikatspeicher**: Für die Authentifizierung bei Windows muss die Zertifizierungsstelle, die Benutzerzertifikate sofort ausstellt (Verkettung wird nicht unterstützt), im NTAuth-Speicher platziert werden. Geben Sie zum Anzeigen dieser Zertifikate im certutil-Programm Folgendes ein: certutil –viewstore –enterprise NTAuth.
- **Speicher für Stamm- und Zwischenzertifikate:** Normalerweise können Zertifikatanmeldesysteme nur ein einzelnes Zertifikat zur Verfügung stellen. Wenn eine Kette verwendet wird, muss daher der Zwischenzertifikatspeicher auf allen Maschinen diese Zertifikate enthalten. Das Stammzertifikat muss im vertrauenswürdigen Stammspeicher und das vorletzte Zertifikat muss im NTAuth-Speicher sein.
- **Anmeldezertifikaterweiterungen und Gruppenrichtlinie:** Windows kann so konfiguriert werden, dass die Überprüfung der EKUs und anderer Zertifikatrichtlinien erzwungen wird. Weitere Informationen finden Sie in der Dokumentation von Microsoft: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

| Registrierungsrichtlinie | Beschreibung |
|---|---|
| AllowCertificatesWithNoEKU | Wenn deaktiviert, müssen Zertifikate die Smartcard-Anmeldung "Erweiterte Schlüsselverwendung" (Enhanced Key Usage, EKU) enthalten. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| AllowSignatureOnlyKeys | Standardmäßig filtert Windows die privaten Schlüssel aus Zertifikaten heraus, die RSA-Entschlüsselung nicht zulassen. Diese Option überschreibt den Filter. |
| AllowTimeInvalidCertificates | Standardmäßig filtert Windows abgelaufene Zertifikate heraus. Diese Option überschreibt den Filter. |
| EnumerateECCCerts | Aktiviert die Authentifizierung mit elliptischen Kurven. |
| X509HintsNeeded | Mit dieser Option können Benutzer ihr Windows-Anmeldekonto manuell angeben, wenn ein Zertifikat keinen eindeutigen Benutzerprinzipalnamen (UPN) enthält oder der Name mehrdeutig ist. |
| UseCachedCRLOnlyAnd<br><br>IgnoreRevocationUnknownErrors | Deaktiviert die Überprüfung von Sperrlisten (normalerweise auf dem Domänencontroller festgelegt). |

- **Domänencontrollerzertifikate**: Zum Authentifizieren von Kerberos-Verbindungen müssen alle Server entsprechende Domänencontrollerzertifikate haben. Diese können mit dem MMC-Snap-In-Menü "Local Computer Certificate Personal Store" angefordert werden.

# Zuordnung von UPN-Namen und Zertifikaten

Es wird empfohlen, dass die Erweiterung des alternativen Antragstellernamens in Benutzerzertifikaten einen eindeutigen UPN (Benutzerprinzipalname) enthält.

**UPN-Namen in Active Directory**

Standardmäßig hat jeder Benutzer in Active Directory eine implizite UPN entsprechend den Mustern @ und @. Die verfügbaren Domänen und FQDNs sind im RootDSE-Eintrag für die Gesamtstruktur enthalten. Für eine einzelne Domäne können mehrere FQDN-Adressen im RootDSE registriert sein.

Darüber hinaus hat jeder Benutzer in Active Directory eine explizite UPN und altUserPrincipalNames. Dies sind LDAP-Einträge, die den UPN für den Benutzer angeben.

Wenn Benutzer anhand der UPN gesucht werden, sucht Windows zuerst in der aktuellen Domäne (basierend auf der Identität des Prozesses bei der Suche nach der UPN) nach expliziten UPNs und dann nach alternativen UPNs. Wenn keine Übereinstimmungen gefunden werden, wird nach der impliziten UPN gesucht, die möglicherweise in anderen Domänen in der Gesamtstruktur aufgelöst wird.

**Zertifikatzuordnungsdienst**


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn ein Zertifikat keine explizite UPN enthält, kann Active Directory für jede Verwendung ein genaues öffentliches Zertifikat in einem "x509certificate"-Attribut speichern. Um ein solches Zertifikat in einen Benutzer aufzulösen, kann ein Computer eine direkte Abfrage für dieses Attribut durchführen (standardmäßig in einer einzelnen Domäne).

Der Benutzer hat die Option, ein Benutzerkonto anzugeben, das die Suche beschleunigt. Dieses Feature kann außerdem in einer domänenübergreifenden Umgebung verwendet werden.

Wenn die Gesamtstruktur mehrere Domänen enthält und der Benutzer eine Domäne nicht explizit angibt, kann der Speicherort des Zertifikatzuordnungsdiensts mit Active Directory rootDSE angegeben werden. Dies ist normalerweise auf einer globalen Katalogmaschine und umfasst die zwischengespeicherte Anzeige aller x509certificate-Attribute in der Gesamtstruktur. Mit diesem Computer kann ein Benutzerkonto basierend auf dem Zertifikat effizient in jeder Domäne gesucht werden.

# Steuern der Domänencontrollerauswahl für die Anmeldung

Wenn eine Umgebung mehrere Domänencontroller umfasst, ist es sinnvoll einzuschränken, welcher Domänencontroller für die Authentifizierung verwendet wird, damit Protokolle aktiviert und abgerufen werden können.

**Steuern der Domänencontrollerauswahl**

Sie können Windows zur Verwendung eines bestimmten Windows-Domänencontrollers für die Anmeldung zwingen, indem Sie durch Konfigurieren der Datei lmhosts eine explizite Liste mit Domänencontrollern festlegen, die eine Windows-Maschine verwendet: \Windows\System32\drivers\etc\lmhosts.

In diesem Speicherort ist normalerweise eine Beispieldatei namens "lmhosts.sam". Fügen Sie einfach eine Zeile hinzu:

```
1.2.3.4   dcnetbiosname #PRE #DOM:mydomain
```

"1.2.3.4" ist die IP-Adresse des Domänencontrollers "dcnetbiosname" in der Domäne "mydomain".

Nach einem Neustart verwendet die Windows-Maschine diese Informationen, um sich bei "mydomain" anzumelden. Diese Konfiguration muss zurückgesetzt werden, wenn das Debuggen abgeschlossen ist.

**Ermitteln des verwendeten Domänencontrollers**

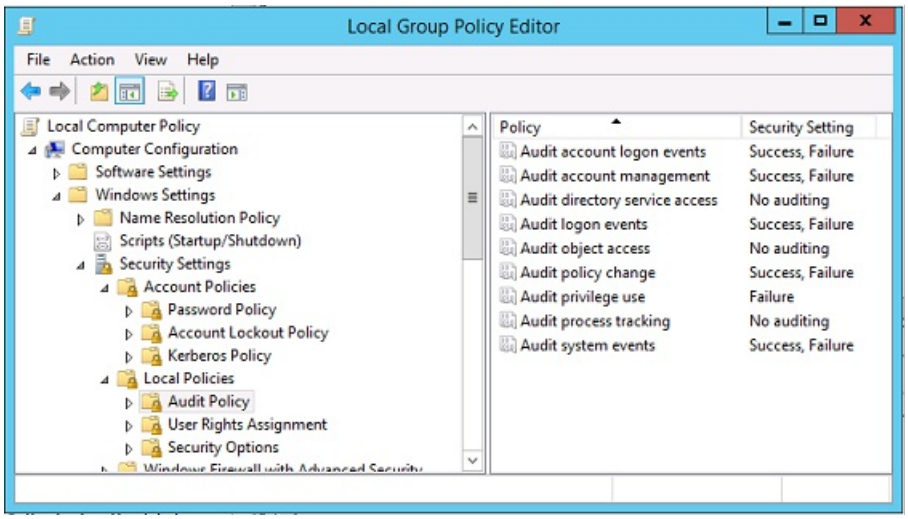
Bei der Anmeldung platziert Windows eine MSDOS-Umgebungsvariable in dem Domänencontroller, der den Benutzer angemeldet hat. Zum Anzeigen starten Sie die Befehlszeile mit dem folgenden Befehl: **echo %LOGONSERVER%**.

Authentifizierungsprotokolle werden auf dem Computer gespeichert, den dieser Befehl zurückgibt.

# Aktivieren von Kontoüberwachungsereignissen

Standardmäßig aktivieren Windows-Domänencontroller keine vollständigen Überwachungsprotokolle für Konten. Überwachungsprotokolle können mit Überwachungsrichtlinien in den Sicherheitseinstellungen im Gruppenrichtlinien-Editor gesteuert werden. Wenn sie aktiviert sind, schreibt der Domänencontroller zusätzliche Ereignisprotokollinformationen in die Protokolldatei.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# Zertifikatüberprüfungsprotokolle

**Zertifikatsgültigkeit überprüfen**

Wenn ein Smartcardzertifikat als DER-Zertifikat (kein privater Schlüssel erforderlich) exportiert wird, können Sie es mit folgendem Befehl überprüfen: certutil –verify user.cer

**CAPI-Protokollierung aktivieren**

Öffnen Sie auf dem Domänencontroller und den Benutzermaschinen die Ereignisanzeige und aktivieren Sie die Protokollierung für Microsoft/Windows/CAPI2/Operational Logs.

Sie können die CAPI-Protokollierung mit den Registrierungsschlüsseln hier steuern: CurrentControlSet\Services\crypt32.

| Wert | Beschreibung |
|---|---|
| DiagLevel (DWORD) | Ausführlichkeitsgrad (0 bis 5) |
| DiagMatchAnyMask (QUADWORD) | Ereignisfilter (0xffffff für alle) |
| DiagProcessName (MULTI_SZ) | Nach Prozessname filtern (z. B. LSASS.exe) |

**CAPI-Protokolle**

| Meldung | Beschreibung |
|---|---|
| Build Chain | LSA-Aufruf: CertGetCertificateChain (einschließlich Ergebnis) |
| Verify Revocation | LSA-Aufruf: CertVerifyRevocation (einschließlich Ergebnis) |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| X509 Objects | Im ausführlichen Modus werden Zertifikate und Zertifikatsperrlisten (CRLs) im Verzeichnis \AppData\LocalLow Microsoft\X509Objects ausgegeben |
| Verify Chain Policy | LSA-Aufruf: CertVerifyChainPolicy (einschließlich Parameter) |

**Fehlermeldungen**

| Fehlercode | Beschreibung |
|---|---|
| Certificate not trusted | Das Smartcardzertifikat konnte nicht mit Zertifikaten aus den Speichern für Zwischenzertifikate und vertrauenswürdige Stammzertifikate erstellt werden. |
| Certificate revocation check error | Die Zertifikatsperrliste für die Smartcard konnte nicht von der Adresse heruntergeladen werden, die vom Zertifikatsperrlisten-Verteilungspunkt angegeben wurde. Wenn die Zertifikatsperrüberprüfung obligatorisch ist, schlagen Anmeldungen fehl. Weitere Informationen finden Sie im Abschnitt Zertifikate und Public Key-Infrastruktur. |
| Certificate Usage errors | Das Zertifikat ist nicht für Anmeldungen geeignet. Es ist möglicherweise ein Serverzertifikat oder ein Signaturzertifikat. |

# Kerberos-Protokolle

Erstellen Sie folgende Registrierungswerte, um Kerberos-Protokollierung auf dem Domänencontroller und der Maschine des Endbenutzers zu aktivieren:

| Struktur | Wertname | Wert [DWORD] |
|---|---|---|
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | LogLevel | 0x1 |
| CurrentControlSet\Control\Lsa\Kerberos\Parameters | KerbDebuglevel | 0xffffffff |
| CurrentControlSet\Services\Kdc | KdcDebugLevel | 0x1 |
| CurrentControlSet\Services\Kdc | KdcExtraLogLevel | 0x1f |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Kerberos-Protokollierung wird im Systemereignisprotokoll aufgezeichnet.

- Meldungen wie "untrusted certificate" sind in der Regel einfach zu diagnostizieren.
- Zwei Fehlercodes sind nur zur Information und können ignoriert werden:
  - KDC_ERR_PREAUTH_REQUIRED (für die Abwärtskompatibilität bei älteren Domänencontrollern)
  - Unknown error 0x4b

# Ereignisprotokollmeldungen

Dieser Abschnitt beschreibt die auf dem Domänencontroller und der Arbeitsstation erwarteten Protokolleinträge, wenn Benutzer sich mit einem Zertifikat anmelden.

- CAPI2-Protokoll des Domänencontrollers
- Sicherheitsprotokoll des Domänencontrollers
- VDA-Sicherheitsprotokoll
- VDA-CAPI-Protokoll
- VDA-Systemprotokoll

## CAPI2-Protokoll des Domänencontrollers

Bei einer Anmeldung überprüft der Domänencontroller das Zertifikat des Aufrufenden, wodurch eine Sequenz von Protokolleinträgen wie nachfolgend dargestellt erstellt wird.

Operational Number of events: 6

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain Policy |
| Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain |
| Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects |
| Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocation |
| Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain |

Die letzte Meldung zeigt, dass lsass.exe auf dem Domänencontroller basierend auf dem vom VDA bereitgestellten Zertifikat eine Kette erstellt und sie auf Gültigkeit überprüft (einschließlich Sperrung). Das zurückgegebene Ergebnis ist "ERROR_SUCCESS".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

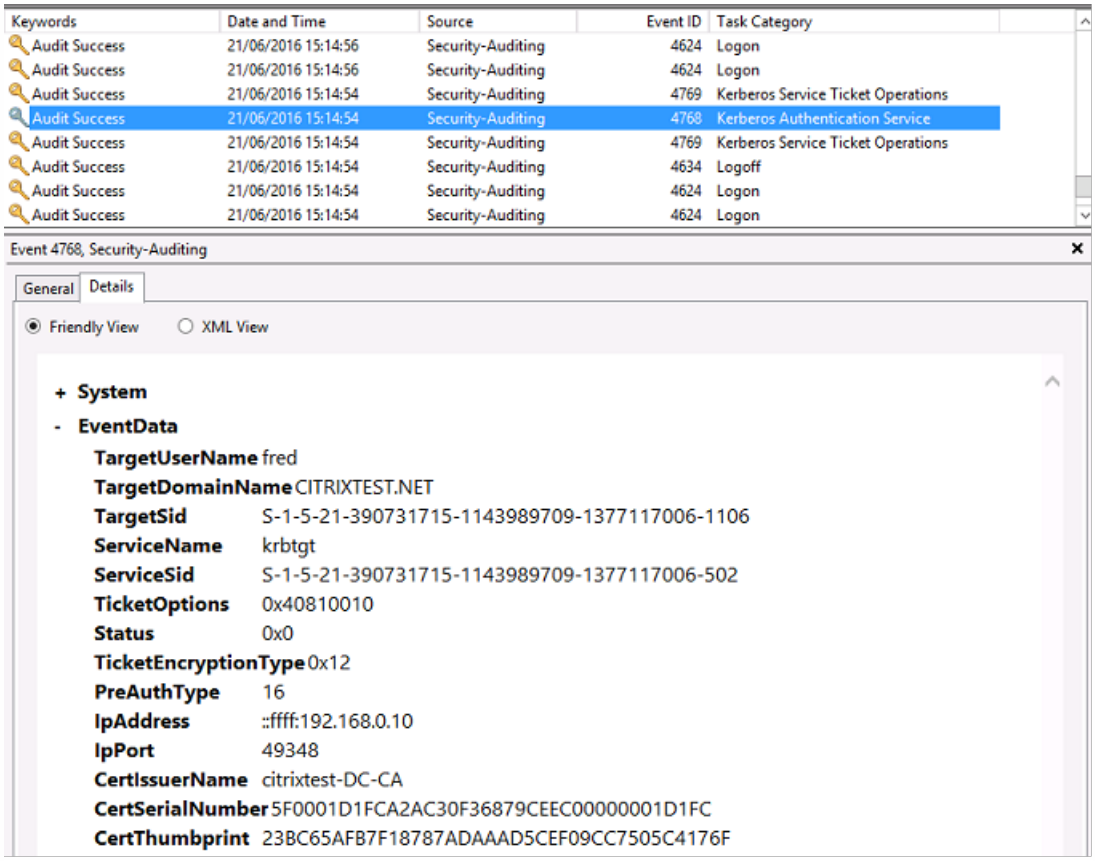
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [ **type**] CERT_CHAIN_POLICY_NT_AUTH
    - [ **constant**] 6
  - **Certificate**
    - [ **fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [ **subjectName**] fred
  - **CertificateChain**
    - [ **chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [ **value**] 0
  - **Status**
    - [ **chainIndex**] -1
    - [ **elementIndex**] -1
  - **EventAuxInfo**
    - [ **ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [ **TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [ **SeqNumber**] 1
  - **Result**
    - [ **value**] 0

## Sicherheitsprotokoll des Domänencontrollers

Der Domänencontroller zeigt eine Reihe von Anmeldeereignissen an, wobei das Ereignis 4768, die Verwendung des Zertifikats zum Ausstellen des Kerberos Ticket Granting Ticket (krbtgt), das wichtigste ist.

Die vorhergehenden Meldungen zeigen, wie sich das Maschinenkonto des Servers beim Domänencontroller authentifiziert. Die darauffolgenden Meldungen zeigen, wie mit dem Benutzerkonto, das nun zum neuen krbtgt gehört, die Authentifizierung beim Domänencontroller durchgeführt wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




## VDA-Sicherheitsprotokoll

Das VDA-Sicherheitsüberwachungsprotokoll, das der Anmeldung entspricht, ist der Eintrag mit der Ereignis-ID 4648, der von winlogon.exe verursacht wurde.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Security Number of events: 24

| Keywords | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4648 | Logon |

Event 4648, Security-Auditing

General | Details

Friendly View | XML View

```
+ System
- EventData
    SubjectUserSid      S-1-5-18
    SubjectUserName     VDA79$
    SubjectDomainName   CITRIXTEST
    SubjectLogonId      0x3e7
    LogonGuid           {00000000-0000-0000-0000-000000000000}
    TargetUserName      fred
    TargetDomainName    CITRIXTEST
    TargetLogonGuid     {51B22BCC-9F90-CE55-6E44-21D7EEC2162C}
    TargetServerName    localhost
    TargetInfo          localhost
    ProcessId           0x126c
    ProcessName         C:\Windows\System32\winlogon.exe
    IpAddress           192.168.0.9
    IpPort              51171
```

## VDA-CAPI-Protokoll

Dieses VDA-CAPI-Beispielprotokoll zeigt eine erstellte Kette und eine Überprüfungssequenz von lsass.exe, mit der das Domänencontrollerzertifikat (dc.citrixtest.net) überprüft wurde.

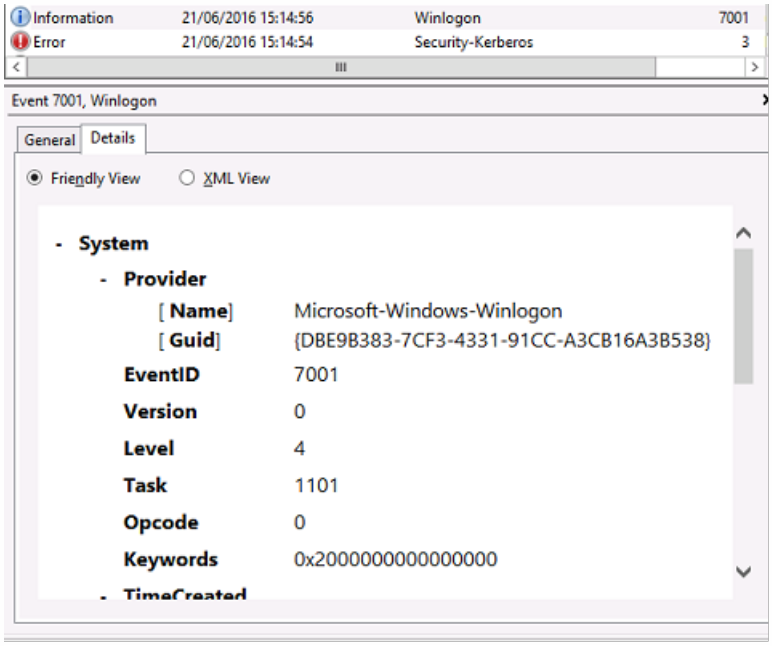
| | | | | |
|---|---|---|---|---|
| Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain P... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain |
| Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects |
| Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocat... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocat... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain |

```
- UserData
  - CertVerifyCertificateChainPolicy
    - Policy
        [type]        CERT_CHAIN_POLICY_NT_AUTH
        [constant]    6
    - Certificate
        [fileRef]     813C6D12E1E1800E61B8DB071E186EB912B7
        [subjectName] dc.citrixtest.net
    - CertificateChain
        [chainRef]    {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - Flags
        [value]       0
    - Status
        [chainIndex]  -1
```

## VDA-Systemprotokoll


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn die Kerberos-Protokollierung aktiviert ist, enthält das Systemprotokoll die Fehlermeldung KDC_ERR_PREAUTH_REQUIRED, die ignoriert werden kann, und einen Eintrag von Winlogon zur erfolgreichen Kerberos-Anmeldung.




# Endbenutzerfehlermeldungen

In diesem Abschnitt finden Sie allgemeine Fehlermeldungen, die Benutzern auf der Windows-Anmeldeseite angezeigt werden.

| Angezeigte Fehlermeldung | Beschreibung und Referenz |
|---|---|
| Ungültiger Benutzername oder Kennwort | Der Computer glaubt, dass Sie ein gültiges Zertifikat und einen gültigen privaten Schlüssel haben, aber der Kerberos-Domänencontroller hat die Verbindung zurückgewiesen. Weitere Informationen finden Sie im Abschnitt Kerberos-Protokolle in diesem Artikel. |
| Sie konnten nicht angemeldet werden. Ihre Anmeldeinformationen konnten nicht überprüft werden.<br><br>Die Anforderung wird nicht unterstützt. | Es kann kein Kontakt zum Domänencontroller hergestellt werden oder auf dem Domänencontroller sind nicht die entsprechenden Zertifikate installiert.<br><br>Registrieren Sie die Zertifikate "Domain Controller" und "Domain Controller Authentication" auf dem Domänencontroller neu, wie in CTX206156 beschrieben. Dies ist einen Versuch wert, selbst wenn die vorhandenen Zertifikate anscheinend gültig sind. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Sie konnten nicht angemeldet werden. Das für die Authentifizierung verwendete Smartcardzertifikat ist nicht vertrauenswürdig. | Die Zwischen- und Stammzertifikate sind nicht auf dem lokalen Computer installiert. Informationen zum Installieren von Smartcardzertifikaten auf nicht in Domänen eingebundenen Computern finden Sie unter CTX206156. Weitere Informationen finden Sie im Abschnitt Zertifikate und Public Key-Infrastruktur in diesem Artikel. |
| Sie können sich nicht anmelden, da die Smartcard-Anmeldung für Ihr Konto nicht unterstützt wird. | Ein Arbeitsgruppenbenutzerkonto wurde für die Smartcard-Anmeldung nicht vollständig konfiguriert. |
| Der angeforderte Schlüssel ist nicht vorhanden. | Ein Zertifikat verweist auf einen privaten Schlüssel, auf den nicht zugegriffen werden kann. Dieser Fall kann eintreten, wenn eine PIV-Karte nicht vollständig konfiguriert ist und die CHUID oder CCC-Datei fehlt. |
| Fehler beim Verwenden der Smartcard | Die Smartcard-Middleware ist nicht ordnungsgemäß installiert. Smartcard-Installationsanweisungen finden Sie unter CTX206156. |
| Smartcard einlegen | Die Smartcard oder der Smartcardleser wurde nicht erkannt. Wenn die Smartcard eingelegt ist, weist diese Meldung auf ein Problem mit der Hardware oder Middleware hin. Smartcard-Installationsanweisungen finden Sie unter CTX206156. |
| Die PIN ist falsch. | Die Smartcard hat die vom Benutzer eingegebene PIN nicht akzeptiert. |
| Es wurde kein gültiges Smartcardzertifikat gefunden. | Die Erweiterungen des Zertifikats sind möglicherweise nicht richtig festgelegt worden oder der RSA-Schlüssel ist zu kurz. (<2048 Bits). Informationen zum Erstellen von gültigen Smartcardzertifikaten finden Sie unter CTX206901. |
| Die Smartcard ist blockiert. | Eine Smartcard wurde gesperrt, z. B. weil der Benutzer mehrmals eine falsche PIN eingegeben hat.<br><br>Ein Administrator hat möglicherweise Zugriff auf den PIN-Entsperrcode (PUK) für die Smartcard und kann die PIN mit einem Tool zurücksetzen, das beim Smartcardhersteller erhältlich ist.<br><br>Wenn der Entsperrcode nicht verfügbar ist oder die |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | Sperrung nicht aufgehoben werden kann, muss die Smartcard auf die Werkseinstellungen zurückgesetzt werden. |
| Ungültige Anforderung | Der private Schlüssel einer Smartcard unterstützt die Kryptografie nicht, die der Domänencontroller erfordert. Beispielsweise fordert der Domänencontroller möglicherweise die Entschlüsselung des privaten Schlüssels, aber die Smartcard unterstützt nur das Signieren.<br><br>Dies weist meist darauf hin, dass die Erweiterungen des Zertifikats nicht ordnungsgemäß festgelegt sind oder dass der RSA-Schlüssel zu kurz ist. (<2048 Bits). Informationen zum Erstellen von gültigen Smartcardzertifikaten finden Sie unter CTX206901. |

# Verwandte Informationen

- Konfigurieren einer Domäne für die Smartcard-Anmeldung: http://support.citrix.com/article/CTX206156
- Smartcard-Anmelderichtlinien: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Aktivieren der CAPI-Protokollierung: http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Aktivieren der Kerberos-Protokollierung: https://support.microsoft.com/en-us/kb/262177
- Richtlinien für die Aktivierung der Smartcard-Anmeldung mit Drittanbieter-Zertifizierungsstellen: https://support.microsoft.com/en-us/kb/281245


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# PowerShell SDK für den Verbundauthentifizierungsdienst

Aug 17, 2016

Die Verwaltungskonsole des Verbundauthentifizierungsdiensts eignet sich für einfache Bereitstellungen, während die PowerShell-Oberfläche erweiterte Optionen bietet. Wenn Sie Optionen verwenden möchten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, ausschließlich PowerShell für die Konfiguration zu verwenden.

Mit dem folgenden Befehl werden die FAS-PowerShell-Cmdlets hinzugefügt:

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

In einem PowerShell-Fenster zeigen Sie mit Get-Help <*cmdlet name*> die Cmdlet-Hilfe an.

Die unter dem Link unten verfügbare ZIP-Datei enthält Hilfedateien für alle Cmdlets des PowerShell SDKs für FAS. Klicken Sie auf den Link, um die ZIP-Datei herunterzuladen. Extrahieren Sie den Inhalt in einen lokalen Ordner. Die Datei index.html enthält eine Liste aller Cmdlets mit Links zu den individuellen Cmdlet-Hilfedateien.

ZIP Hilfedateien für PowerShell-Cmdlets für den Verbundauthentifizierungsdienst


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Drucken

Jul 15, 2016

Die Druckerverwaltung in Ihrer Umgebung umfasst verschiedene Stufen:

1. Machen Sie sich, falls erforderlich, mit den Druckkonzepten vertraut.
2. Planen der Druckarchitektur. Dazu gehört die Analyse folgender Faktoren: Unternehmensanforderungen, vorhandene Druckinfrastruktur, derzeitige Interaktion von Benutzern und Anwendungen mit Druckvorgängen und das für Ihre Umgebung am besten geeignete Druckverwaltungsmodell.
3. Konfigurieren Sie die Druckumgebung, indem Sie eine Druckerbereitstellungsmethode auswählen und dann Richtlinien zur Bereitstellung Ihres Druckkonzepts erstellen. Aktualisieren Sie Richtlinien, wenn neue Mitarbeiter oder Server hinzugefügt werden.
4. Testen einer Druckkonfiguration, bevor sie den Benutzern bereitgestellt wird.
5. Pflegen Sie die Citrix Druckumgebung durch Verwalten von Druckertreibern und Optimieren der Druckleistung.
6. Beseitigen Sie evtl. auftretende Probleme.

## Druckkonzepte

Bevor Sie die Bereitstellung planen, sollten Sie mit folgenden Hauptkonzepten des Druckens vertraut sein:

- Arten der Druckerbereitstellung
- Wie Druckaufträge weitergeleitet werden
- Grundlagen der Druckertreiberverwaltung

Die Druckkonzepte bauen auf denen von Windows auf. Um das Drucken in Ihrer Umgebung zu konfigurieren und erfolgreich zu verwalten, müssen Sie verstehen, wie das Netzwerk- und Clientdrucken in Windows funktioniert und wie das Druckverhalten in dieser Umgebung umgesetzt wird.

## Ablauf des Druckprozesses

In dieser Umgebung werden alle Druckvorgänge (durch den Benutzer) auf Maschinen initiiert, auf denen Anwendungen gehostet werden. Druckaufträge werden über den Netzwerkdruckserver oder das Benutzergerät an das Druckgerät weitergeleitet.

Wenn ein Benutzer druckt, übernimmt das System folgende Aufgaben:

- Entscheidung darüber, welche Drucker dem Benutzer bereitgestellt werden. Dies wird als Druckerprovisioning bezeichnet.
- Wiederherstellen der Druckeinstellungen des Benutzers.
- Ermitteln des Standarddruckers für die Sitzung.

Sie können festlegen, wie diese Aufgaben durchgeführt werden, indem Sie die Optionen für das Druckerprovisioning, die Weiterleitung von Druckaufträgen, das Speichern von Druckereigenschaften und die Treiberverwaltung konfigurieren. Bedenken Sie dabei, wie die verschiedenen Einstellungen möglicherweise die Druckleistung in der Umgebung und die Benutzererfahrung beeinflussen.

## Druckerprovisioning

Der Prozess, durch den Drucker in einer Sitzung verfügbar gemacht werden, wird als Provisioning bezeichnet. Das Druckerprovisioning wird normalerweise dynamisch abgewickelt. Das heißt, die in einer Sitzung angezeigten Drucker sind nicht vordefiniert und gespeichert. Stattdessen werden die Drucker gemäß der Richtlinien beim Entstehen der Sitzung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

während der Anmeldung und Wiederverbindung zusammengestellt. Folglich können sich die Drucker je nach Richtlinie, Benutzerort und Netzwerkänderungen ändern, vorausgesetzt, dies spiegelt sich in den Richtlinien wider. Benutzer, die an einen anderen Ort wechseln, bemerken daher möglicherweise Änderungen in ihrem Arbeitsbereich.

Das System überwacht auch clientseitige Drucker und passt automatisch erstellte Drucker in Sitzungen dynamisch an, je nachdem, welche Hinzufügungen, Löschungen und Änderungen an den clientseitigen Druckern vorgenommen werden. Von dieser dynamischen Druckerermittlung profitieren mobile Benutzer, wenn sie über verschiedene Geräte eine Verbindung herstellen.

Die gängigsten Methoden der Druckerbereitstellung sind folgende:

- **Universeller Druckserver**: Der universelle Druckserver von Citrix bietet universelle Druckunterstützung für Netzwerkdrucker. Der universelle Druckserver verwendet den universellen Druckertreiber. Diese Lösung ermöglicht die Verwendung eines einzelnen Treibers auf einer Serverbetriebssystemmaschine und damit den Netzwerkdruck von jedem Gerät aus.

  Citrix empfiehlt den Einsatz des universellen Druckservers für Szenarios mit Remote-Druckerservern. Der universelle Druckserver überträgt den Druckauftrag über das Netzwerk in einem optimierten und komprimierten Format, wodurch der Netzwerkverkehr reduziert und die Benutzererfahrung verbessert wird.

  Der universelle Druckserver umfasst als Feature die folgenden Komponenten:

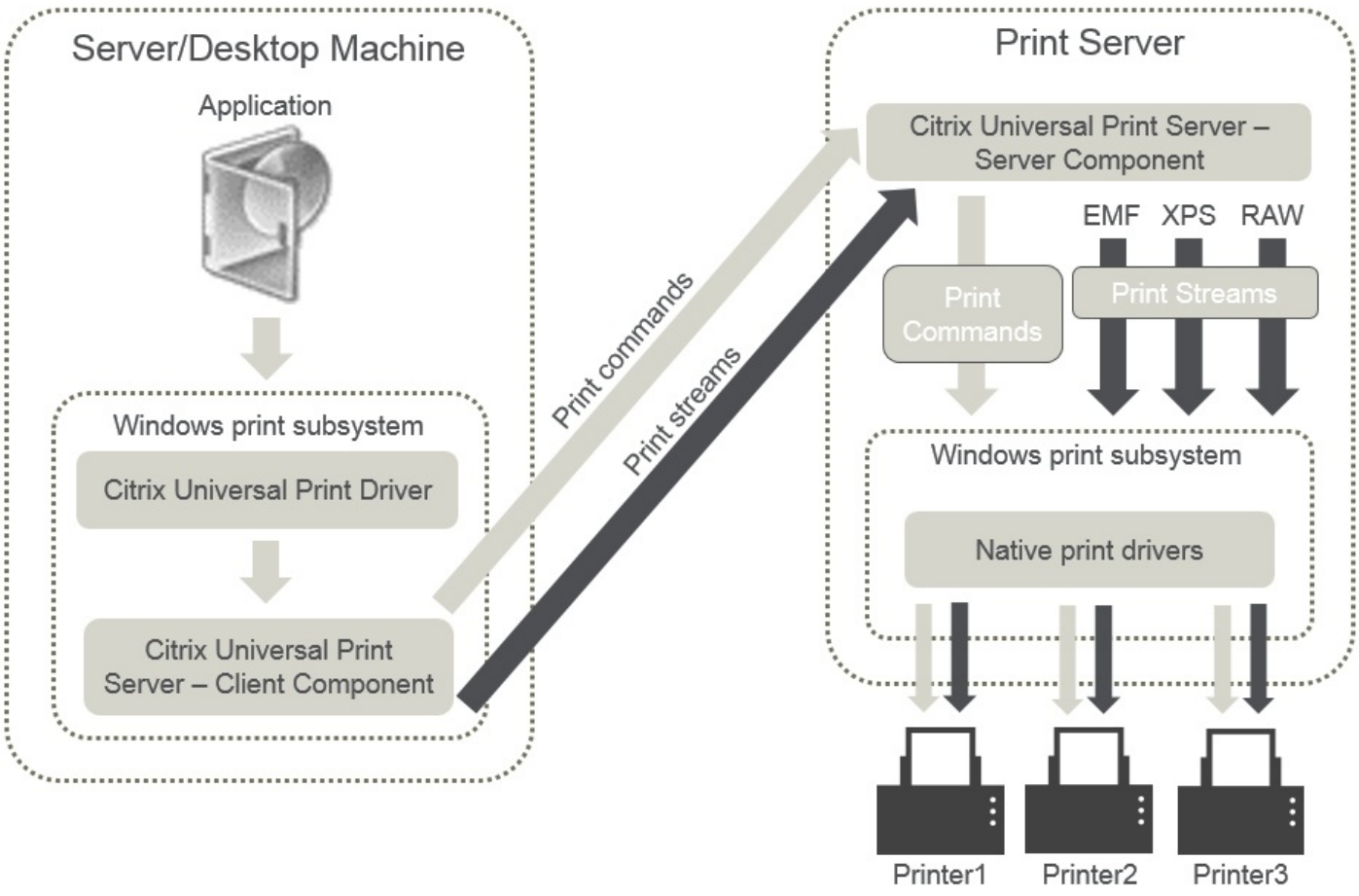
  Clientkomponente **UPClient**: Aktivieren Sie UPClient auf jeder Serverbetriebssystemmaschine, die Netzwerksitzungsdrucker bereitstellt und den universellen Druckertreiber verwendet.

  Serverkomponente **UPServer**: Installieren Sie UPServer auf jedem Druckserver, der Netzwerksitzungsdrucker bereitstellt und den universellen Druckertreiber für die Sitzungsdrucker verwendet (unabhängig davon, ob die Sitzungsdrucker zentral bereitgestellt werden).

Informationen zu den Anforderungen und zum Setup des universellen Druckservers finden Sie in den Artikeln Systemanforderungen und Installation.

Die folgende Abbildung zeigt den typischen Workflow eines Netzwerkdruckers in einer Umgebung mit universellem Druckserver.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Wenn Sie das Citrix Feature "Universeller Druckserver" aktivieren, wird es von allen verbundenen Netzwerkdruckern automatisch über Autodiscovery genutzt.

**Hinweis:** Der universelle Druckserver wird auch für VDI-in-a-Box 5.3 unterstützt. Informationen zur Installation des universellen Druckservers mit VDI-in-a-Box finden Sie in der Dokumentation zu VDI-in-a-Box.

- **Automatische Erstellung**: Dies bezieht sich auf Drucker, die automatisch zu Beginn jeder Sitzung erstellt werden. Sowohl Remotedrucker als auch lokal angeschlossene Drucker können automatisch erstellt werden. Bei Umgebungen mit einer großen Anzahl von Druckern pro Benutzer ist es u. U. besser, nur den Standarddrucker automatisch zu erstellen. Wenn weniger Drucker automatisch erstellt werden, entsteht auf den Serverbetriebssystemmaschinen weniger Mehraufwand (Arbeitsspeicher und CPU). Eine reduzierte Anzahl an automatisch erstellten Druckern kann auch die Anmeldedauer der Benutzer verkürzen.
  Automatisch erstellte Drucker basieren auf:

  - Den auf dem Benutzergerät installierten Druckern.
  - Den auf die Sitzung angewendeten Richtlinien.
    Durch Richtlinieneinstellungen für die automatische Erstellung können Sie Anzahl oder Art der automatisch erstellten Drucker beschränken. Standardmäßig sind die Drucker in Sitzungen verfügbar, wenn alle Drucker auf dem Benutzergerät automatisch konfiguriert werden, einschließlich der lokal angeschlossenen und der Netzwerkdrucker.

  Nachdem der Benutzer die Sitzung beendet, werden die Drucker für diese Sitzung gelöscht.

  Mit der automatischen Erstellung von Client- und Netzwerkdruckern sind Wartungsarbeiten verbunden. Bei Hinzufügen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

eines Druckers muss beispielsweise auch Folgendes durchgeführt werden:

- Aktualisieren der Richtlinieneinstellung "Sitzungsdrucker"
- Hinzufügen des Treibers zu allen Serverbetriebssystemmaschinen über die Richtlinieneinstellung "Druckertreiberzuordnung und -kompatibilität"

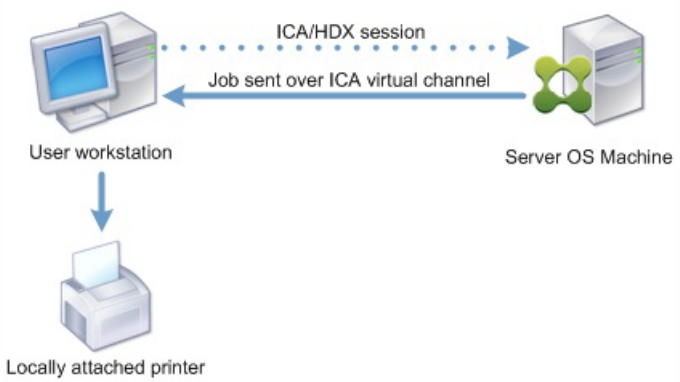
## Weiterleiten von Druckaufträgen

Der Begriff Druckpfad umfasst den Pfad, über den Druckaufträge weitergeleitet werden, und den Speicherort, an dem Druckaufträge gespoolt werden. Beide Aspekte dieses Konzepts sind wichtig. Die Weiterleitung wirkt sich auf den Netzwerk-Datenverkehr aus. Das Spooling wirkt sich auf die Auslastung der lokalen Ressourcen an dem Gerät, das den Auftrag verarbeitet, aus.

In dieser Umgebung können Druckaufträge auf zwei Wegen zu einem Druckgerät gelangen: über den Client oder über einen Netzwerkdruckserver. Dafür werden die Bezeichnungen Clientdruckpfad und Netzwerkdruckpfad verwendet. Welcher Pfad standardmäßig ausgewählt wird, hängt vom verwendeten Drucker ab.

**Lokal angeschlossene Drucker**

Das System leitet Aufträge von der Serverbetriebssystemmaschine über den Client an den Drucker. Der Druckdatenverkehr wird über das ICA-Protokoll optimiert und komprimiert. Wenn ein Druckgerät lokal an das Benutzergerät angeschlossen ist, werden Druckaufträge über den virtuellen ICA-Kanal weitergeleitet.




**Netzwerkdrucker**

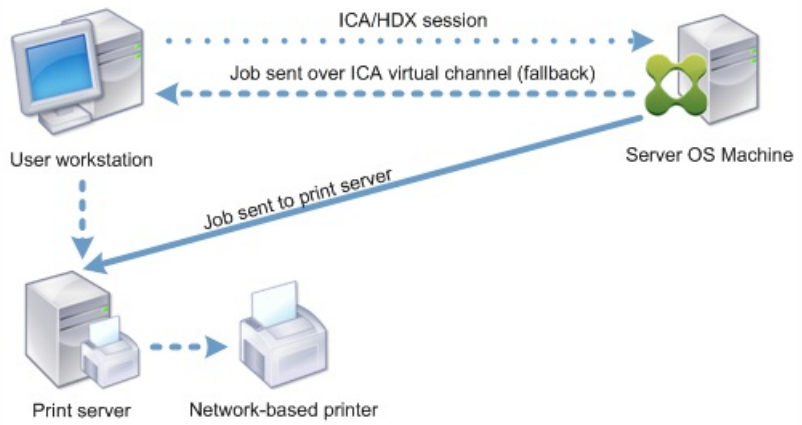
Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. In folgenden Situationen werden jedoch Druckaufträge automatisch über die ICA-Verbindung geleitet:

- Wenn der virtuelle Desktop oder die Anwendung keine Verbindung mit dem Druckserver herstellen kann.
- Wenn der systemeigene Druckertreiber auf der Serverbetriebssystemmaschine nicht verfügbar ist.

Wenn der universelle Druckserver nicht aktiviert ist, empfiehlt sich die Konfiguration des Clientdruckpfads für den Netzwerkdruck bei Verbindungen mit geringer Bandbreite, z. B. WANs, die von der Optimierung und Komprimierung des Datenverkehrs beim Senden von Aufträgen über die ICA-Verbindung profitieren.

Der Clientdruckpfad ermöglicht auch die Begrenzung des Datenverkehrs oder der für Druckaufträge zugeordneten Bandbreite. Wenn die Auftragsleitung über das Benutzergerät nicht möglich ist, z. B. bei Thin Clients ohne Druckerfunktionen, muss die Servicequalität so konfiguriert werden, dass ICA/HDX-Verkehr Vorrang hat und eine gute Benutzererfahrung bei der Sitzung gewährleistet ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

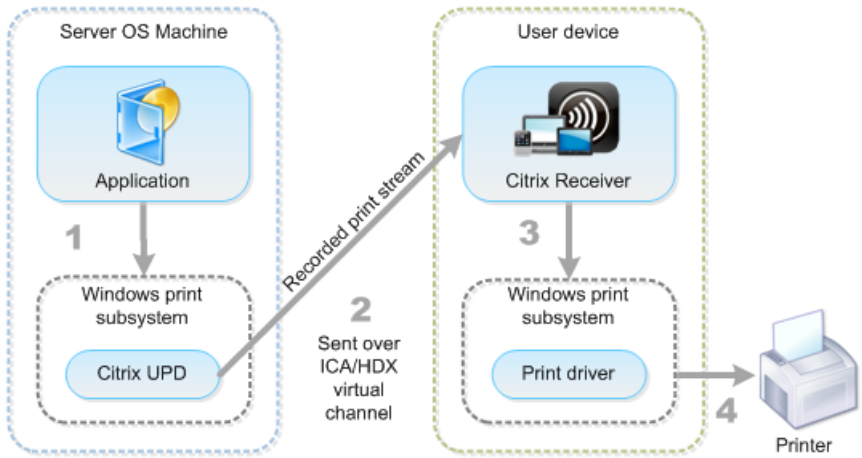



## Druckertreiberverwaltung

Zur Vereinfachung der Druckprozesse in dieser Umgebung empfiehlt Citrix die Verwendung des universellen Citrix Druckertreibers. Der universelle Druckertreiber ist ein geräteunabhängiger, für jedes Druckgerät geeigneter Treiber. Durch die so erzielte Reduzierung der Treiberanzahl wird die Verwaltung erheblich vereinfacht.

Der universelle Citrix XPS-Druckertreiber unterstützt erweiterte Druckerfunktionen, wie Heftung und Auswahl der Papierzufuhr. Die Funktionen sind verfügbar, wenn sie durch den nativen Treiber über Microsoft Print Capability zur Verfügung gestellt werden. Der native Treiber muss die standardisierten Druckschemastichwörter in der XML-Datei mit den Druckfunktionen verwenden. Werden nicht standardmäßige Stichwörter verwendet, stehen die erweiterten Druckfunktionen über den universellen Citrix XPS-Druckertreiber nicht zur Verfügung.

Die folgende Abbildung zeigt die universellen Druckertreiberkomponenten und einen typischen Workflow für ein lokal angeschlossenes Druckgerät.

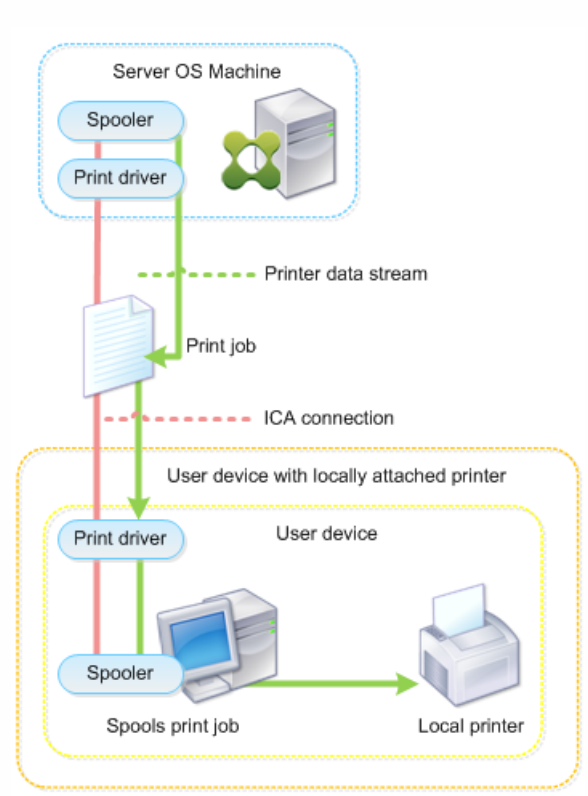



Legen Sie bei der Planung der Strategie zur Treiberverwaltung fest, ob Sie gerätespezifische Treiber, den universellen Druckertreiber oder beides unterstützen wollen. Wenn Sie Standardtreiber unterstützen, müssen Sie außerdem Folgendes festlegen:

Wenn das System während der automatischen Druckererstellung erkennt, dass ein neuer lokaler Drucker an einem Benutzergerät angeschlossen ist, wird die Serverbetriebssystemmaschine auf den erforderlichen Druckertreiber hin überprüft. Ist kein Windows-systemeigener Treiber verfügbar, wird vom System standardmäßig der universelle Druckertreiber verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Der Druckvorgang kann nur dann erfolgreich ausgeführt werden, wenn der Druckertreiber auf der Serverbetriebssystemmaschine und der Treiber auf dem Benutzergerät übereinstimmen. In der folgenden Abbildung wird dargestellt, wie der Druckertreiber an zwei Orten für den Clientdruck verwendet wird.




- Zu unterstützende Treibertypen
- Aktivieren oder Deaktivieren der automatischen Installation der Druckertreiber (falls auf Serverbetriebssystemmaschinen nicht vorhanden)
- Erstellen der Treiberkompatibilitätslisten

## Verwandter Inhalt

- Beispiel einer Druckkonfiguration
- Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge
- Druckrichtlinien und Einstellungen
- Bereitstellen von Druckern
- Pflege der Druckumgebung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Beispiel einer Druckkonfiguration

Jul 08, 2016

Die Auswahl der am besten geeigneten Druckkonfigurationsoptionen für die Anforderungen und die Umgebung kann die Verwaltung vereinfachen. Obwohl die Standarddruckkonfiguration für die meisten Umgebungen geeignet ist, gewährleisten die Standardwerte möglicherweise nicht die erwartete Benutzererfahrung oder die optimale Netzwerkverwendung und den gewünschten Verwaltungsaufwand für die Umgebung.

Die Druckkonfiguration hängt von folgenden Faktoren ab:

- Den Unternehmensanforderungen und der vorhandenen Druckinfrastruktur.
  Berücksichtigen Sie bei der Druckkonfiguration die Anforderungen der Organisation. Die vorhandene Druckimplementierung (ob Benutzer Drucker hinzufügen können, welche Benutzer Zugriff auf welche Drucker haben usw.) kann bei der Definition der Druckkonfiguration ein nützlicher Leitfaden sein.
- Ob in Ihrer Organisation Sicherheitsrichtlinien gelten, die Drucker für bestimmte Benutzer reservieren (z. B. Drucker für die Personalabteilung oder die Gehaltsabrechnung).
- Ob Benutzer drucken müssen, wenn sie nicht an ihrem primären Arbeitsort sind, z. B. Mitarbeiter, die verschiedene Arbeitsstationen verwenden oder auf Geschäftsreisen gehen.

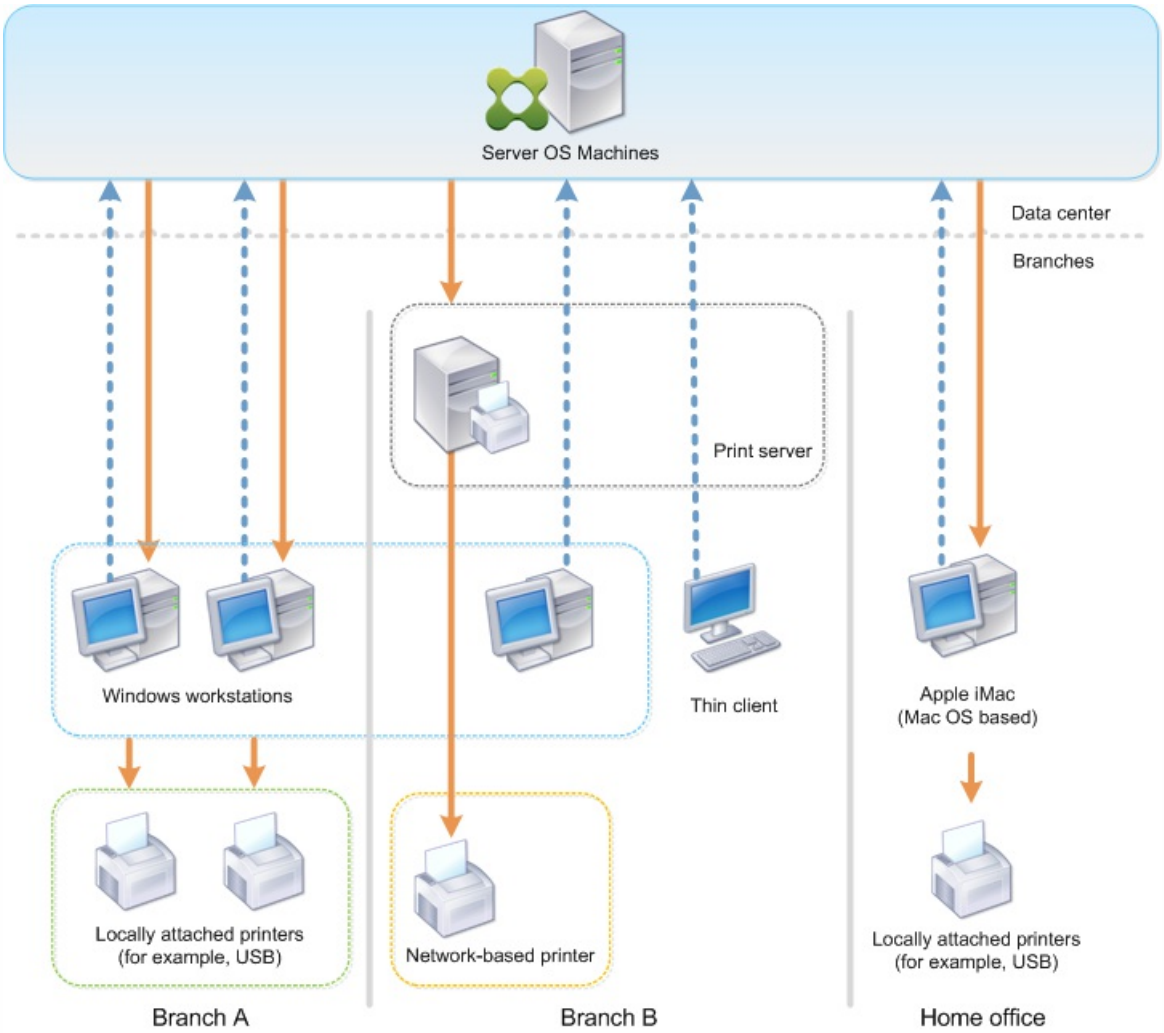
Achten Sie beim Entwerfen der Druckkonfiguration darauf, den Benutzern die gleiche Erfahrung in einer Sitzung zu bieten, wie sie es beim Drucken von lokalen Benutzergeräten aus gewohnt sind.

## Beispiel einer Druckbereitstellung

Die folgende Abbildung zeigt die Bereitstellung dieser Anwendungsfälle:

- **Zweigstelle A**: Kleine Auslandsniederlassung mit einigen Windows-Arbeitsstationen. Jede Benutzerarbeitsstation hat einen lokal angeschlossenen, privaten Drucker.
- **Zweigstelle B**: Großes Zweigstellenbüro mit Thin Clients und auf Windows basierenden Arbeitsstationen. Aus Effizienzgründen teilen sich die Benutzer dieser Zweigstelle die Netzwerkdrucker (einen pro Stockwerk). Die Druckwarteschlangen werden über Windows-Druckserver der Zweigstelle gesteuert.
- **Home Office**: Büro im Haus eines Mitarbeiters mit einem Mac OS-basierten Benutzergerät, über das auf die Citrix Infrastruktur des Unternehmens zugegriffen wird. Das Benutzergerät hat einen lokal angeschlossenen Drucker.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




In den folgenden Abschnitten werden Konfigurationen beschrieben, die die Komplexität der Umgebung minimieren und die Verwaltung vereinfachen.

## Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

In Branch A arbeiten alle Benutzer auf Arbeitsstationen unter Windows und verwenden daher automatisch erstellte Clientdrucker und den universellen Druckertreiber. Dies bietet folgende Vorteile:

- Leistung: Druckaufträge werden über den ICA-Druckkanal geleitet, sodass die Druckdaten komprimiert werden können und Bandbreite eingespart wird.
  Um sicherzustellen, dass ein einzelner Benutzer durch den Druck eines großen Dokuments nicht die Sitzungsleistung anderer Benutzer beeinträchtigt, wird eine Citrix Richtlinie für die maximale Druckbandbreite konfiguriert.

  Eine andere Lösung wäre die Multistream-ICA-Verbindung, bei der der Druckverkehr innerhalb einer separaten TCP-Verbindung mit niedriger Priorität übertragen wird. Multistream-ICA kann verwendet werden, wenn Quality of Service (QoS) über die WAN-Verbindung nicht implementiert ist.

- Flexibilität: Der universelle Citrix Druckertreiber gewährleistet, dass alle mit dem Client verbundenen Drucker auch von virtuellen Desktop- oder Anwendungssitzungen verwendet werden können, ohne dass ein neuer Druckertreiber im Datencenter integriert werden muss.

## Universeller Citrix Druckserver

In Branch B werden alle Netzwerkdrucker und ihre Warteschlangen auf einem Windows-Druckerserver verwaltet. Somit


© 1999-2017 Citrix Systems, Inc. All rights reserved.

erweist sich der universelle Citrix Druckserver als die effizienteste Konfiguration.

Alle erforderlichen Druckertreiber werden von lokalen Administratoren auf dem Druckserver installiert und verwaltet. Das Zuordnen von Druckern in virtuellen Desktop- oder Anwendungssitzungen funktioniert wie folgt:

- Arbeitsstationen unter Windows: Das IT-Team vor Ort hilft den Benutzern beim Herstellen der Verbindung zwischen ihren Windows-Arbeitsstationen und dem geeigneten Netzwerkdrucker. Dies ermöglicht Benutzern, über lokal installierte Anwendungen zu drucken.
  Bei virtuellen Desktop- oder Anwendungssitzungen werden die lokal konfigurierten Drucker über die automatische Erstellung aufgelistet. Der virtuelle Desktop oder die virtuelle Anwendung stellt dann eine Verbindung mit dem Druckserver her, falls möglich, als Direktnetzwerkverbindung.

  Die Komponenten des universellen Citrix Druckservers werden installiert und aktiviert, systemeigene Druckertreiber sind nicht erforderlich. Falls ein Treiber aktualisiert oder eine Druckerwarteschlange geändert wird, ist im Datencenter keine weitere Konfiguration nötig.

- Thin Clients: Für Thin Clients-Benutzer müssen die Drucker in den virtuellen Desktop- oder Anwendungssitzungen angeschlossen werden. Um den Benutzern das Drucken so einfach wie möglich zu machen, konfigurieren die Administratoren eine einzige Citrix Sitzungsdruckerrichtlinie pro Stockwerk, damit der jeweilige Drucker als Standarddrucker festgelegt wird.
  Damit sichergestellt ist, dass die Benutzer stets mit dem richtigen Drucker verbunden sind, auch wenn sie in einem anderen Stockwerk sind, werden die Richtlinien nach Subnetz oder Thin Client-Namen gefiltert. Diese Konfiguration, die auch als "Proximitydrucken" bezeichnet wird, lässt die Wartung lokaler Druckertreiber zu (gemäß der delegierten Administration).

  Wenn eine Druckerwarteschlange geändert oder hinzugefügt werden muss, müssen Citrix Administratoren die entsprechende Richtlinie für Sitzungsdrucker in der Umgebung ändern.

Da der Netzwerkdruckdatenverkehr außerhalb des virtuellen ICA-Kanals gesendet wird, wird QoS implementiert. Eingehende und ausgehende Netzwerkdaten an Ports für ICA/HDX-Datenverkehr haben Vorrang vor sonstigem Netzwerkdatenverkehr. Diese Konfiguration gewährleistet, dass Benutzersitzungen von großen Druckaufträgen nicht beeinträchtigt werden.

### Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

Bei Heimbüros mit nicht standardmäßigen Arbeitsstationen und nicht verwalteten Druckgeräten ist es am einfachsten, automatisch erstellte Drucker und den universellen Druckertreiber zu verwenden.

### Zusammenfassung der Bereitstellung

Zusammenfassend lässt sich die Konfiguration dieses Bereitstellungsbeispiels wie folgt beschreiben:

- Auf Serverbetriebssystemmaschinen werden keine Druckertreiber installiert. Es wird nur der universelle Citrix Druckertreiber verwendet. Fallback auf systemeigene Druckertreiber und die automatische Installation von Druckertreibern sind deaktiviert.
- Die automatische Erstellung von Clientdruckern für alle Benutzer wird über eine Richtlinie konfiguriert. Serverbetriebssystemmaschinen werden standardmäßig direkt mit dem Druckserver verbunden. Zur Konfiguration müssen lediglich die Komponenten des universellen Druckservers aktiviert werden.
- Eine Sitzungsdruckerrichtlinie wird für jedes Stockwerk von Branch B konfiguriert und gilt für alle Thin Clients des jeweiligen Stockwerks.
- Die Implementierung von QoS für Branch B gewährleistet eine hervorragende Benutzererfahrung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge

Jul 08, 2016

## Bewährte Methoden

Viele Faktoren bestimmen die beste Drucklösung für eine bestimmte Umgebung. Einige dieser bewährten Methoden sind möglicherweise für Ihre Site nicht geeignet.

- Verwenden Sie das Citrix Feature "universeller Druckserver".
- Verwenden Sie den universellen Druckertreiber oder Windows-systemeigene Treiber.
- Reduzieren Sie die Anzahl der installierten Druckertreiber auf den Serverbetriebssystemmaschinen auf das Minimum.
- Verwenden Sie Treiberzuordnung zu systemeigenen Treibern.
- Installieren Sie nie ungetestete Druckertreiber in einer Produktionssite.
- Vermeiden Sie Updates von Treibern. Versuchen Sie stets, einen Treiber zu deinstallieren, den Server neu zu starten und dann einen Ersatztreiber zu installieren.
- Deinstallieren Sie nicht verwendete Treiber oder verwenden Sie die Richtlinie Druckertreiberzuordnung und -kompatibilität, um zu verhindern, dass Drucker mit dem Treiber erstellt werden.
- Vermeiden Sie möglichst Kernelmodustreiber der Version 2.
- Wenden Sie sich an den Hersteller oder sehen Sie in der Citrix Ready-Produktdokumentation www.citrix.com/ready nach, ob ein Druckermodell unterstützt wird.
  Im Allgemeinen werden alle von Microsoft zur Verfügung gestellten Druckertreiber mit Terminaldiensten getestet und ihre Funktion unter Citrix gewährleistet. Vergewissern Sie sich jedoch vor Einsatz eines Druckertreibers eines Drittanbieters, dass der Treiber von Windows Hardware Quality Labs (WHQL) für Terminaldienste zertifiziert wurde. Citrix vergibt keine Zertifizierung für Druckertreiber.

## Sicherheitsüberlegungen

Citrix Drucklösungen sind inhärent sicher.

- Der Citrix Druckmanagerdienst überwacht und reagiert fortlaufend auf Sitzungsereignisse wie An- und Abmeldung, Trennen, Wiederverbinden und Beenden der Sitzung. Er behandelt Anforderungen, indem er die Identität des Benutzers der aktuellen Sitzung übernimmt.
- Beim Citrix Drucken wird jedem Drucker ein eindeutiger Namespace in einer Sitzung zugewiesen.
- Die Standardsicherheitsbeschreibung für automatisch erstellte Drucker wird eingerichtet, um sicherzustellen, dass die in einer Sitzung automatisch erstellten Clientdrucker für Benutzer in anderen Sitzungen nicht zugänglich sind. Standardmäßig können Administratoren nicht versehentlich auf einem Clientdrucker einer anderen Sitzung drucken, obwohl sie jeden Clientdrucker sehen und die Berechtigungen dafür manuell ändern können.

## Standarddruckvorgänge

Wenn Sie keine Richtlinienregeln konfigurieren, zeigt sich standardmäßig das folgende Druckverhalten:

- Universeller Druckserver ist deaktiviert.
- Alle auf dem Benutzergerät konfigurierten Drucker werden automatisch zu Beginn jeder Sitzung konfiguriert. Dieses Verhalten entspricht der Richtlinieneinstellung Clientdrucker automatisch erstellen mit der Option Alle Clientdrucker automatisch erstellen.

- Das System leitet alle Druckaufträge, die in Warteschlangen für an Benutzergeräte lokal angeschlossene Drucker gestellt wurden, als Clientdruckaufträge weiter (d. h. über den ICA-Kanal und durch das Benutzergerät).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Das System leitet alle Druckaufträge, die in Warteschlangen von Netzwerkdruckern gestellt wurden, direkt über Serverbetriebssystemmaschinen. Falls die Aufträge vom System nicht über das Netzwerk weitergeleitet werden können, werden sie als umgeleiteter Clientdruckauftrag über das Benutzergerät weitergeleitet.
  Dieses Verhalten entspricht dem Deaktivieren der Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern.

- Standardmäßig versucht das System, die Druckeigenschaften (eine Kombination aus den Druckeinstellungen des Benutzers und den gerätespezifischen Druckeinstellungen) auf dem Benutzergerät zu speichern. Wenn der Client diesen Vorgang nicht unterstützt, werden die Druckeigenschaften vom System in Benutzerprofilen auf der Serverbetriebssystemmaschine gespeichert.
  Dieses Verhalten entspricht der Citrix Richtlinieneinstellung Speicherung von Druckereigenschaften mit der Option Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind.

- Das System verwendet die Windows-Version des Druckertreibers, falls sie auf der Serverbetriebssystemmaschine verfügbar ist. Ist der Druckertreiber nicht verfügbar, versucht das System, den Treiber vom Windows-Betriebssystem zu installieren. Ist der Treiber in Windows nicht verfügbar, wird ein universeller Citrix Druckertreiber verwendet.
  Dieses Verhalten entspricht dem Aktivieren der Citrix Richtlinieneinstellung Automatische Installation von mitgelieferten Druckertreibern und Konfigurieren der Einstellung Universal Printing mit der Option Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist.

  Das Aktivieren von Automatische Installation von mitgelieferten Druckertreibern kann dazu führen, dass eine große Anzahl systemeigener Druckertreiber installiert wird.

Hinweis: Wenn Sie nicht sicher sind, welche Standardwerte voreingestellt sind, zeigen Sie sie an, indem Sie eine neue Richtlinie erstellen und alle Druckrichtlinienregeln aktivieren. Die angezeigte Option ist die Standardoption.

## Immer aktive Protokollierung

Eine Always-On-Protokollierung ist für den Druckserver und das Drucksubsystem auf dem VDA verfügbar.

Zum Sortieren der Protokolle als ZIP-Datei für den E-Mail-Versand bzw. für den automatischen Upload an Citrix Insight Services verwenden das PowerShell-Cmdlet **Start-TelemetryUpload**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Druckrichtlinien und -einstellungen

Jul 08, 2016

Wenn Benutzer von veröffentlichten Anwendungen aus auf Drucker zugreifen, können Sie über Citrix Richtlinien Folgendes konfigurieren:

- Wie das Drucker-Provisioning erfolgt (bzw. wie Drucker zu Sitzungen hinzugefügt werden)
- Wie Druckaufträge weitergeleitet werden
- Wie Druckertreiber verwaltet werden

Sie können verschiedene Druckkonfigurationen für unterschiedliche Benutzergeräte, Benutzer oder beliebige andere Objekte haben, nach denen Richtlinien gefiltert werden.

Die meisten Druckfunktionen werden über die Citrix Druckrichtlinieneinstellungen konfiguriert. Druckeinstellungen folgen dem Standardverhalten von Citrix Richtlinien.

Druckereinstellungen können vom System am Ende einer Sitzung in das Druckerobjekt oder das Clientdruckgerät geschrieben werden, sofern das Netzwerkkonto des Benutzers ausreichende Berechtigungen hat. Standardmäßig verwendet Citrix Receiver die Einstellungen, die im Druckerobjekt in der Sitzung gespeichert wurden, bevor an anderen Orten nach Einstellungen gesucht wird.

Standardmäßig werden die Druckereigenschaften auf dem Benutzergerät (falls vom Gerät unterstützt) oder im Benutzerprofil auf der Serverbetriebssystemmaschine gespeichert oder beibehalten. Wenn die Druckereigenschaften während einer Sitzung vom Benutzer geändert werden, werden diese Änderungen im Benutzerprofil auf der Maschine aktualisiert. Wenn sich der Benutzer das nächste Mal anmeldet oder eine neue Verbindung herstellt, übernimmt das Benutzergerät die beibehaltenen Einstellungen. Das heißt, auf dem Benutzergerät geänderte Druckereigenschaften wirken sich nicht auf die aktuelle Sitzung aus bis zum Ab- und erneuten Anmelden des Benutzers.

## Speicherorte für Druckeinstellungen

In Windows-Druckumgebungen können die an den Druckvoreinstellungen vorgenommenen Änderungen auf dem lokalen Computer oder in einem Dokument gespeichert werden. Wenn Benutzer in dieser Umgebung Druckeinstellungen ändern, können diese Änderungen an folgenden Positionen gespeichert werden:

- **Auf dem Benutzergerät**: Windows-Benutzer können Geräteeinstellungen auf dem Benutzergerät ändern, indem sie mit der rechten Maustaste auf die Drucker in der Systemsteuerung klicken und Druckeinstellungen wählen. Wenn beispielsweise Querformat als Seitenausrichtung ausgewählt wird, gilt Querformat als Standard-Seitenausrichtung für diesen Drucker.
- **In einem Dokument**: Bei Textverarbeitungs- und Desktop-Publishing-Programmen werden Dokumenteinstellungen, z. B. die Seitenausrichtung, häufig in Dokumenten gespeichert. Wenn Sie beispielsweise ein zu druckendes Dokument in eine Warteschlange setzen, speichert Microsoft Word die von Ihnen angegebenen Druckvoreinstellungen wie Seitenausrichtung und Druckername im Dokument selbst. Diese Einstellungen erscheinen standardmäßig, wenn Sie dieses Dokument das nächste Mal drucken.
- **Benutzerseitige Änderungen in einer Sitzung**: Das System übernimmt Änderungen an den Druckeinstellungen eines automatisch erstellten Druckers nur, wenn diese in der Systemsteuerung der Sitzung vorgenommen wurden, also auf der Serverbetriebssystemmaschine.
- **Auf der Serverbetriebssystemmaschine**: Dies sind die Standardeinstellungen, die einem bestimmten Druckertreiber auf der Maschine zugeordnet sind.

Die in einer Windows-Umgebung gespeicherten Einstellungen sind abhängig von der Stelle, an der die Einstellungen vom


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Benutzer vorgenommen wurden. Das bedeutet außerdem, dass die an einer Stelle wie einer Tabellenkalkulation angezeigten Druckeinstellungen sich von den Einstellungen an anderen Stellen, beispielsweise in Dokumenten, unterscheiden können. Die auf einen bestimmten Drucker angewendeten Druckeinstellungen variieren daher innerhalb einer Sitzung.

### Hierarchie der Benutzerdruckeinstellungen

Da die Druckeinstellungen an verschiedenen Stellen gespeichert werden können, verarbeitet das System sie gemäß einer bestimmten Priorität. Sie dürfen auch nicht vergessen, dass Geräteeinstellungen anders behandelt werden als Dokumenteinstellungen und normalerweise Vorrang vor diesen haben.

Standardmäßig wendet das System immer alle Druckeinstellungen an, die ein Benutzer während einer Sitzung geändert hat, d. h. alle beibehaltenen Einstellungen, bevor andere Einstellungen berücksichtigt werden. Wenn der Benutzer druckt, führt das System die auf der Serverbetriebssystemmaschine gespeicherten Standarddruckereinstellungen mit allen beibehaltenen Einstellungen oder Clientdruckeinstellungen zusammen und wendet sie an.

### Speichern der Druckeinstellungen des Benutzers

Citrix empfiehlt, dass Sie den Speicherort der Druckereigenschaften nicht ändern. Am einfachsten können Sie konsistente Druckereigenschaften sicherstellen, indem Sie die Standardeinstellung beibehalten, wonach die Druckereigenschaften auf dem Benutzergerät gespeichert werden. Wenn das System die Eigenschaften auf dem Benutzergerät nicht speichern kann, wird automatisch auf das Benutzerprofil auf der Serverbetriebssystemmaschine zurückgegriffen.

Überprüfen Sie die Richtlinieneinstellung Speicherung von Druckereigenschaften, wenn diese Szenarios zutreffen:

- Verwendung von älteren Plug-Ins, durch die das Speichern der Druckereigenschaften durch die Benutzer auf einem Benutzergerät unterbunden wird
- Verwendung verbindlicher Profile im Windows-Netzwerk, wobei die Druckereigenschaften der Benutzer beibehalten werden sollen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Bereitstellen von Druckern

Jul 15, 2016

Es gibt drei Methoden der Druckerbereitstellung:

- Universeller Citrix Druckserver
- Automatisch erstellte Clientdrucker
- Vom Administrator zugewiesene Sitzungsdrucker

### Universeller Citrix Druckserver

Bei der Wahl der besten Drucklösung für Ihre Umgebung sollten Sie Folgendes berücksichtigen:

- Der universelle Druckserver bietet Features, die beim Windows-Druckanbieter nicht verfügbar sind: Zwischenspeichern von Bildern und Schriftarten, erweiterte Komprimierung, Optimierung und Unterstützung für QoS.
- Der universelle Druckertreiber unterstützt die von Microsoft definierten, öffentlichen geräteunabhängigen Einstellungen. Wenn Benutzer Zugriff auf die Geräteeinstellungen des Druckertreibers eines bestimmten Herstellers benötigen, stellt der universelle Druckserver gepaart mit einem Windows-systemeigenen Treiber die beste Lösung dar. In dieser Konfiguration bleiben die Vorteile des universellen Druckservers erhalten und die Benutzer können zugleich auf bestimmte Druckerfunktionen zugreifen. Allerdings ist zu bedenken, dass Windows-systemeigene Treiber wartungsbedürftig sind.
- Der universelle Druckserver von Citrix bietet universelle Druckunterstützung für Netzwerkdrucker. Der universelle Druckserver verwendet den universellen Druckertreiber, einen einzelnen Treiber auf der Serverbetriebssystemmaschine, mit dem von jedem Gerät aus, einschließlich Thin Clients und Tablets, auf lokalen oder Netzwerkdruckern gedruckt werden kann.

Um den universellen Druckserver mit einem Windows-systemeigenen Treiber zu verwenden, aktivieren Sie den universellen Druckserver. Wenn der Windows-systemeigene Treiber verfügbar ist, wird er standardmäßig verwendet. Andernfalls wird der universelle Druckertreiber verwendet. Um dieses Verhalten zu ändern, beispielsweise zur ausschließlichen Verwendung des Windows-systemeigenen Treibers oder des universellen Druckertreibers, müssen Sie die Richtlinieneinstellung Verwendung universeller Druckertreiber aktualisieren.

## Installieren des universellen Druckservers

Zum Verwenden des universellen Druckservers installieren Sie die UPsServer-Komponente, wie in den Dokumenten zur Installation beschrieben, auf den Druckservern und konfigurieren Sie sie. Weitere Informationen finden Sie unter Installieren über die grafische Oberfläche und Installieren über die Befehlszeile.

In Umgebungen, in denen Sie die UPClient-Komponente separat bereitstellen, z. B. mit **XenApp 6.5**:

1. Laden Sie das eigenständige Paket für den XenApp und XenDesktop Virtual Delivery Agent (VDA) für Windows-Desktopbetriebssysteme oder Windows-Serverbetriebssysteme herunter.
2. Extrahieren Sie den VDA gemäß den Anweisungen für die Befehlszeile unter Verwenden des dedizierten VDA-Installationsprogramms.
3. Installieren Sie die Voraussetzungen aus \Image-Full\Support\VcRedist_2013_RTM
   - Vcredist_x64 / vcredist_x86
     - Führen Sie x86 nur bei 32-Bit-Bereitstellungen aus und beide bei 64-Bit-Bereitstellungen
4. Installieren Sie die CDF-Voraussetzung aus \Image-Full\x64\Virtual Desktop Components oder \Image-Full\x86\Virtual Desktop Components.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cdf_x64 / Cdf_x86
  - x86 für 32 Bit, x64 für 64 Bit
5. Navigieren Sie zur UPClient-Komponente in \Image-Full\x64\Virtual Desktop Components oder in \Image-Full\x86\Virtual Desktop Components.
6. Installieren Sie die UPClient-Komponente, indem Sie die MSI der Komponente extrahieren und starten.
7. Nach der Installation der UPClient-Komponente ist ein Neustart erforderlich.

## Deaktivieren der Teilnahme am CEIP für den universellen Druckserver

Bei der Installation des universellen Druckservers werden Sie automatisch für das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) registriert. Der erste Upload von Daten erfolgt sieben Tage nach der Installation.

Zum Deaktivieren der Teilnahme am CEIP legen Sie den **DWORD**-Wert des Registrierungsschlüssels **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** auf **0** fest.

Wenn Sie anschließend wieder teilnehmen möchten, legen Sie den DWORD-Wert auf 1 fest.

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Weitere Informationen finden Sie unter Citrix Insight Services.

## Konfigurieren des universellen Druckservers

Verwenden Sie die folgenden Citrix Richtlinieneinstellungen zum Konfigurieren des universellen Druckservers. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.

- **Universellen Druckserver aktivieren**: Der universelle Druckserver ist standardmäßig deaktiviert. Wenn Sie ihn aktivieren, müssen Sie festlegen, ob der Windows-Druckanbieter verwendet werden soll, wenn der universelle Druckserver nicht verfügbar ist. Nachdem der universelle Druckserver aktiviert wurde, können Benutzer Netzwerkdrucker über die Windows-Druckanbieter- und Citrix Anbieteroberflächen hinzufügen und auflisten.
- **Port für Druckdatenstrom des universellen Druckservers (CGP)**: Nummer des TCP-Ports, die vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet wird. Standardwert: **7229**.
- **Port für universellen Druckserverwebdienst (HTTP/SOAP)**: Nummer des Standard-TCP-Ports, der vom Listener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen verwendet wird. Standardwert: **8080**.

Zum Ändern des HTTP-Standardports 8080 für die Kommunikation zwischen universellem Druckserver und XenApp- bzw. XenDesktop-VDAs müssen Sie außerdem auf Computern mit dem universeller Druckserver den folgenden Registrierungsschlüssel erstellen und die Portnummer ändern:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
"UpsHttpPort"=DWORD:

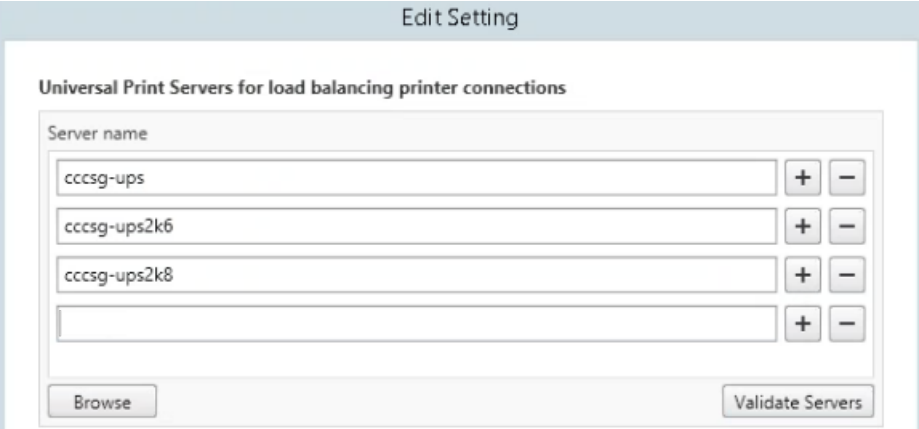
Diese Portnummer muss mit dem Port für den universellen Druckserverwebdienst (HTTP/SOAP) der HDX-Richtlinie in Studio übereinstimmen.

- **Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)**: gibt das obere Limit (in Kilobit pro Sekunde) für die Übertragungsrate der Druckdaten an, die von jedem Druckauftrag mit CGP an den universellen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Druckserver übergeben werden. Standardwert: 0 (unbegrenzt).

- **Universelle Druckserver für den Lastausgleich**: Mit dieser Einstellung werden die universellen Druckserver aufgelistet, die zum Lastausgleich für am Sitzungsstart erstellte Druckerverbindungen verwendet werden, nachdem andere Citrix Druckrichtlinieneinstellungen bewertet wurden. Zum Optimieren der Erstellungszeit von Druckern empfiehlt Citrix, dass alle Druckserver über denselben Satz freigegebener Drucker verfügen. Klicken Sie auf **Server überprüfen**, um zu prüfen, ob die einzelnen Server Druckserver sind, und um sicherzustellen, dass auf allen Druckservern ein identischer Satz freigegebener Drucker installiert ist. Dieser Vorgang kann einige Zeit dauern.




- **Außer-Betrieb-Schwellenwert für universelle Druckserver**: Gibt an, wie lange der Load Balancer auf die Wiederherstellung eines nicht verfügbaren Druckservers warten muss, bevor er den Server als bleibend offline einstuft und dessen Last auf andere verfügbare Druckserver verteilt. Standardwert ist 180 (Sekunden).

Nach Ändern von Druckrichtlinien auf dem Delivery Controller kann es einige Minuten dauern, bis die Änderungen auf die VDAs angewendet werden. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Universeller Druckserver".

**Interaktion mit anderen Richtlinieneinstellungen**: Der universelle Druckserver berücksichtigt andere Citrix Druckrichtlinieneinstellungen und interagiert mit diesen (siehe folgende Tabelle). Die Angaben basieren auf folgender Annahme: Die Richtlinieneinstellung "Universeller Druckserver" ist aktiviert, die Komponenten des universellen Druckservers sind installiert und die Richtlinieneinstellungen werden angewendet.

| Richtlinieneinstellung | Interaktion |
|---|---|
| Clientdruckerumleitung, automatisches Erstellen von Clientdruckern | Wenn der universelle Druckserver aktiviert ist, werden Clientnetzwerkdrucker mit dem universellen Druckertreiber statt den systemeigenen Treibern erstellt. Den Benutzern wird der gleiche Druckername wie zuvor angezeigt. |
| Sitzungsdrucker | Wenn Sie die Citrix Lösung des universellen Druckservers einsetzen, werden die Richtlinieneinstellungen für universelle Druckertreiber berücksichtigt. |
| Direkte Verbindungen zu Druckserver | Wenn der universelle Druckserver aktiviert ist und die Einstellung für die Richtlinie "Verwendung universeller Druckertreiber" für die ausschließliche Verwendung des universellen Druckens konfiguriert ist, |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

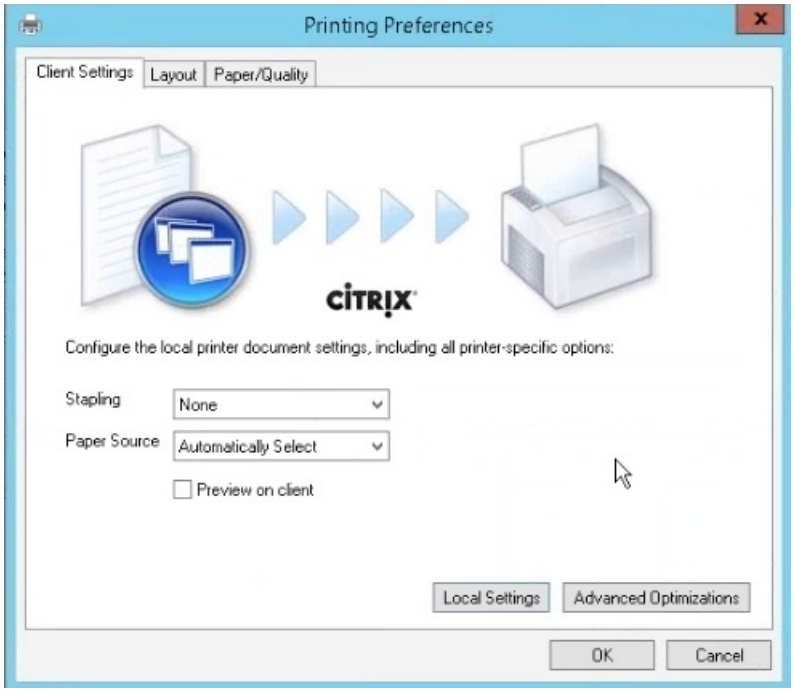
| | |
|---|---|
| | kann mit dem universellen Druckertreiber ein direkter Netzwerkdrucker zum Druckserver erstellt werden. |
| UPD-Präferenz | Unterstützt EMF- und XPS-Treiber. |

**Auswirkungen auf Benutzeroberflächen**: Der vom universellen Druckserver verwendete universelle Citrix Druckertreiber deaktiviert die folgenden Benutzeroberflächensteuerelemente:

- Schaltfläche für die lokalen Druckereinstellungen im Druckereigenschaften-Dialogfeld
- Schaltflächen für die lokalen Druckereinstellungen und die Vorschau im Dokumenteigenschaften-Dialogfeld

Der universelle Citrix XPS-Druckertreiber unterstützt erweiterte Druckfunktionen, wie z. B. Heftung und Auswahl der Druckmaterialquelle. Die Benutzer können die Optionen für Heften und Druckmaterialquelle im benutzerdefinierten UPD-Druckdialogfeld wählen, wenn die dem UPD für die Sitzung zugewiesenen Client- bzw. Netzwerkdrucker die Features unterstützen.

Die Funktionen sind verfügbar, wenn sie durch den nativen Treiber über Microsoft Print Capability zur Verfügung gestellt werden. Der native Treiber muss die standardisierten Druckschemastichwörter in der XML-Datei mit den Druckfunktionen verwenden. Werden nicht standardmäßige Stichwörter verwendet, stehen die erweiterten Druckfunktionen über den universellen Citrix XPS-Druckertreiber nicht zur Verfügung.




Beim universellen Druckserver gleicht der Assistent für die Druckerinstallation des Citrix Druckanbieters dem für den Windows-Druckanbieter mit den folgenden Ausnahmen:

- Beim Hinzufügen eines Druckers mit dem Namen oder einer Adresse können Sie eine HTTP/SOAP-Portnummer für den Druckserver angeben. Die Portnummer wird Teil des Druckernamens und wird angezeigt.
- Wenn in der Einstellung für die Richtlinie "Verwendung universeller Druckertreiber" festgelegt ist, dass universelles Drucken verwendet werden muss, wird der Name des universellen Druckertreibers bei der Auswahl des Druckers


© 1999-2017 Citrix Systems, Inc. All rights reserved.

angezeigt. Der Windows-Druckanbieter kann den universellen Druckertreiber nicht verwenden.

Der Citrix Druckanbieter unterstützt kein clientseitiges Rendering.

Weitere Informationen zum universellen Druckserver finden Sie unter CTX200328.

### Automatisch erstellte Clientdrucker

Die folgenden universellen Drucklösungen sind für Clientdrucker verfügbar:

- **Citrix Universeller Drucker**: ein generischer Drucker, der zu Beginn einer Sitzung erstellt wird und nicht an ein Druckgerät gebunden ist. Der Citrix Universelle Drucker muss die verfügbaren Clientdrucker bei der Anmeldung nicht auflisten, wodurch sich der Ressourceneinsatz erheblich reduziert und die Anmeldedauer für die Benutzer verringert wird. Mit dem Citrix Universellen Drucker kann auf jedem clientseitigen Druckgerät gedruckt werden.
  Der Citrix Universelle Drucker funktioniert allerdings möglicherweise nicht für alle Benutzergeräte oder Citrix Receiver in Ihrer Umgebung. Der Citrix Universelle Drucker erfordert eine Windows-Umgebung und unterstützt nicht das Citrix Offline Plug-In oder Anwendungen, die an Clients gestreamt werden. Verwenden Sie für solche Umgebungen automatisch erstellte Drucker und den universellen Druckertreiber.

  Wenn Sie eine universelle Drucklösung für Citrix Receiver benötigen, die nicht unter Windows ausgeführt werden, verwenden Sie einen der anderen universellen PostScript/PCL-Druckertreiber, die automatisch installiert werden.

- **Citrix Universeller Druckertreiber:** ein geräteunabhängiger Druckertreiber. Wenn Sie einen universellen Citrix Druckertreiber einrichten, verwendet das System standardmäßig den auf EMF basierenden universellen Druckertreiber. Der universelle Citrix Druckertreiber kann auch kleinere Druckaufträge erstellen als ältere oder weniger umfangreiche Druckertreiber. Für Spezialdrucker wird jedoch u. U. ein gerätespezifischer Treiber benötigt, um die Druckaufträge optimal zu verarbeiten.

**Konfigurieren von Universal Printing**: Verwenden Sie die folgenden Citrix Richtlinieneinstellungen zum Konfigurieren von Universal Printing. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.

- Verwenden universeller Druckertreiber: Mit dieser Einstellung legen Sie fest, wann das universelle Drucken verwendet wird.
- Automatisch generischen universellen Drucker erstellen: Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen mit einem Benutzergerät, das mit Universal Printing kompatibel ist. Standardmäßig werden generische universelle Drucker nicht automatisch erstellt.
- Priorität universeller Treiber: Mit dieser Einstellung geben Sie an, in welcher Reihenfolge das System die universellen Druckertreiber verwendet, angefangen mit dem ersten Eintrag in der Liste. Sie können Treiber hinzufügen, bearbeiten oder entfernen und die Reihenfolge der Treiber in der Liste ändern.
- Universelles Drucken - Vorschaueinstellung Mit dieser Einstellung geben Sie an, ob die Druckvorschau für automatisch erstellte oder universelle Drucker verwendet werden soll.
- Universelles Drucken - EMF-Verarbeitungsmodus Mit dieser Einstellung steuern Sie die Verarbeitungsmethode für die EMF-Spooldatei auf dem Windows-Benutzergerät. Standardmäßig werden EMF-Datensätze direkt zum Drucker gespoolt. Direktes Spoolen an den Drucker ermöglicht eine schnellere Verarbeitung der Datensätze durch den Spooler und beansprucht weniger CPU-Ressourcen.

Weitere Richtlinien finden Sie unter Optimieren der Druckleistung. Informationen zum Ändern der Standardeinstellungen (Papierformat, Druckqualität, Farbe, Seitenaufdruck und Auflage) finden Sie unter CTX113148.

**Drucker automatisch über das Benutzergerät erstellen**: Zu Beginn einer Sitzung erstellt das System standardmäßig alle Drucker auf dem Benutzergerät automatisch. Sie können steuern, welche Typen der Drucker ggf. den Benutzern bereitgestellt werden und somit ein automatisches Erstellen verhindern.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Verwenden Sie die Citrix Richtlinieneinstellung Clientdrucker automatisch erstellen, um das automatische Erstellen zu steuern. Sie können Folgendes festlegen:

- Alle für das Benutzergerät sichtbaren Drucker, einschließlich der Netzwerkdrucker und der lokal angeschlossenen Drucker, werden zu Beginn einer Sitzung automatisch erstellt (Standardeinstellung)
- Alle lokalen Drucker, die physisch an das Benutzergerät angeschlossen sind, werden automatisch erstellt
- Nur der Standarddrucker für das Benutzergerät wird automatisch erstellt
- Automatische Erstellung ist für alle Clientdrucker deaktiviert

Die Einstellung Clientdrucker automatisch erstellen erfordert, dass für die Einstellung Clientdruckerumleitung Zugelassen (Standardeinstellung) festgelegt ist.

### Zuweisen von Netzwerkdruckern an Benutzer

Standardmäßig werden die Netzwerkdrucker auf dem Benutzergerät automatisch zu Beginn jeder Sitzung konfiguriert. Sie können die Anzahl der aufgelisteten und zugeordneten Netzwerkdrucker reduzieren, indem Sie festlegen, welche Netzwerkdrucker in jeder Sitzung erstellt werden sollen. Diese Drucker werden als Sitzungsdrucker bezeichnet.

Sie können die Sitzungsdruckerrichtlinien nach IP-Adressen filtern, um das Proximitydrucken (auf dem nächstgelegenen Drucker) zu gewährleisten. Das Drucken auf dem nächstgelegenen Drucker ermöglicht den Benutzern innerhalb eines angegebenen IP-Adressbereichs den automatischen Zugriff auf Netzwerkdruckgeräte, die im gleichen Bereich liegen. Proximitydrucken wird von der Funktion Citrix Universeller Druckserver umgesetzt; die hier beschriebene Konfiguration ist dazu nicht erforderlich.

Proximitydrucken kann folgende Szenarios umfassen:

- Das interne Unternehmensnetzwerk nutzt einen DHCP-Server, der automatisch IP-Adressen für Benutzer zuweist.
- Alle Abteilungen im Unternehmen haben eindeutige zugeordnete IP-Adressbereiche.
- In den IP-Adressbereichen jeder Abteilung gibt es Netzwerkdrucker.

Wenn Proximitydrucken konfiguriert ist und ein Mitarbeiter einer Abteilung in eine andere wechselt, ist keine zusätzliche Druckgerätekonfiguration erforderlich. Sobald das Benutzergerät im IP-Adressbereich der neuen Abteilung erkannt wird, erhält es Zugriff auf alle Netzwerkdrucker in diesem Bereich.

**Konfigurieren bestimmter Drucker für die Umleitung in Sitzungen**: Zum Erstellen von Administratoren zugewiesener Drucker konfigurieren Sie die Citrix Richtlinieneinstellung Sitzungsdrucker. Verwenden Sie zum Hinzufügen eines Netzwerkdruckers zu dieser Richtlinie eine der folgenden Methoden:

- Geben Sie den UNC-Pfad im Format \\servername\printername ein.
- Navigieren Sie zu einem Drucker im Netzwerk.
- Navigieren Sie zu Druckern auf einem bestimmten Server. Geben Sie den Servernamen im Format \\servername an und klicken Sie auf Durchsuchen.

Wichtig: Der Server führt alle aktivierten Einstellungen für Sitzungsdrucker für alle angewendeten Richtlinien zusammen, angefangen von der höchsten bis zur niedrigsten Priorität. Ist ein Drucker in mehreren Richtlinienobjekten konfiguriert, werden angepasste Standardeinstellungen nur aus dem Richtlinienobjekt mit der höchsten Priorität verwendet, in dem der Drucker konfiguriert ist.
Welche Netzwerkdrucker über die Einstellung Sitzungsdrucker erstellt werden, kann je nachdem, wo die Sitzung gestartet wurde, durch Filtern nach Objekten, z. B. Subnetzen, variieren.

**Festlegen eines Standardnetzwerkdruckers für eine Sitzung**: Standardmäßig wird der Hauptdrucker des Benutzers als Standarddrucker für eine Sitzung verwendet. Verwenden Sie die Citrix Richtlinieneinstellung Standarddrucker, um die Auswahl des Standarddruckers auf dem Benutzergerät in einer Sitzung zu ändern.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie unter Standarddrucker eine Einstellung für Standarddrucker des Clients wählen:
   - Netzwerkdruckername: Drucker, die mit der Richtlinieneinstellung Sitzungsdrucker hinzugefügt wurden, werden in diesem Menü angezeigt. Wählen Sie den als Standard für diese Richtlinie zu verwendenden Netzwerkdrucker aus.
   - Standarddrucker des Benutzers nicht anpassen: Verwendet die Einstellung der Terminaldienste oder des aktuellen Benutzerprofils für den Standarddrucker. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.
2. Wenden Sie die Richtlinie auf die Benutzergruppe (oder andere gefilterte Objekte) an, auf die sich auswirken soll.

**Konfigurieren von Proximitydrucken:** Das Proximitydrucken (Drucken auf dem nächstgelegenen Drucker) wird ebenfalls über den universellen Druckserver von Citrix bereitgestellt. Dieser erfordert nicht die hier beschriebene Konfiguration.

1. Erstellen Sie eine separate Richtlinie für jedes Subnetz (oder entsprechend dem Druckerstandort).
2. Fügen Sie in jeder Richtlinie der Einstellung Sitzungsdrucker die Drucker an dem geografischen Standort des Subnetzes hinzu.
3. Setzen Sie die Einstellung Standarddrucker auf Standarddrucker des Benutzers nicht anpassen.
4. Filtern Sie die Richtlinien nach Client-IP-Adresse. Aktualisieren Sie diese Richtlinien, um Änderungen der DHCP-IP-Adressbereiche zu berücksichtigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Pflege der Druckumgebung

Jul 08, 2016

Zur Pflege der Druckumgebung gehört Folgendes:

- Verwalten von Druckertreibern
- Optimieren der Druckleistung
- Anzeigen von Druckern und Verwalten von Druckwarteschlangen

## Verwalten von Druckertreibern

Citrix empfiehlt die Verwendung des universellen Citrix Druckertreibers, um den Verwaltungsaufwand und mögliche Probleme mit Druckertreibern gering zu halten.

Wenn die automatische Erstellung fehlschlägt, installiert das System standardmäßig einen bei Windows integrierten systemeigenen Druckertreiber. Falls kein Treiber verfügbar ist, greift das System automatisch auf den universellen Druckertreiber zurück. Weitere Informationen über Druckertreiber-Standardwerte finden Sie unter Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge.

Wenn der universelle Druckertreiber von Citrix nicht für alle Szenarios geeignet ist, reduzieren Sie die Anzahl installierter Treiber auf Serverbetriebssystemmaschinen mit von Druckertreiberzuordnungen. Außerdem bietet die Zuordnung von Druckertreibern folgende Optionen:

- Beschränken bestimmter Drucker auf die ausschließliche Verwendung des universellen Citrix Druckertreibers
- Zulassen oder Verhindern der Erstellung von Druckern mit einem bestimmten Treiber
- Ersetzen veralteter oder beschädigter Treiber durch gewünschte Druckertreiber
- Ersetzen von Clienttreibernamen durch einen unter Windows Server verfügbaren Treiber

**Automatische Installation von Druckertreibern verhindern**: Die automatische Installation von Druckertreibern muss deaktiviert sein, damit Konsistenz zwischen Serverbetriebssystemmaschinen gewährleistet ist. Dies kann über Citrix Richtlinien und/oder Microsoft-Richtlinien erreicht werden. Zum Verhindern der automatischen Installation Windows-systemeigener Druckertreiber deaktivieren Sie die Citrix Richtlinieneinstellung Automatische Installation von mitgelieferten Druckertreibern.

**Zuordnen von Clientdruckertreibern**: Jeder Client liefert bei der Anmeldung Informationen zu den clientseitigen Druckern, einschließlich dem Namen des Druckermodells. Bei der automatischen Erstellung der Clientdrucker werden die Namen der Druckertreiber auf dem Windows-Server ausgewählt, die den Namen der Druckermodelle entsprechen, die der Client bereitgestellt hat. Beim automatischen Erstellen werden mit diesen identifizierten verfügbaren Druckertreibern umgeleitete Clientdruckwarteschlangen erstellt.

Gehen Sie bei der Erstellung von Regeln für die Treiberersetzung und der Bearbeitung der Druckeinstellungen für zugeordnete Clientdruckertreiber grundsätzlich folgendermaßen vor:

1. Legen Sie die Regeln für die Treiberersetzung für automatisch erstellte Drucker fest, indem Sie die Citrix Richtlinieneinstellung Druckertreiberzuordnung und -kompatibilität konfigurieren. Fügen Sie dabei den Namen des Clientdruckertreibers hinzu und wählen Sie über das Menü Druckertreiber suchen den Servertreiber aus, durch den Sie den Clientdruckertreiber ersetzen möchten. Sie können in dieser Einstellung Platzhalter verwenden. Damit beispielsweise alle HP-Drucker einen bestimmten Treiber verwenden, geben Sie in der Richtlinieneinstellung HP* an.
2. Zum Ausschließen eines Druckertreibers wählen Sie den Namen des Treibers aus und aktivieren Sie die Einstellung Nicht erstellen.
3. Sie können bei Bedarf eine Treiberzuordnung bearbeiten, eine Zuordnung löschen oder die Reihenfolge der


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Treibereinträge in der Liste ändern.

4. Zum Bearbeiten der Druckeinstellungen für zugeordnete Clientdruckertreiber wählen Sie den Druckertreiber aus, klicken Sie auf Einstellungen und geben Sie die Einstellungen wie Druckqualität, Ausrichtung und Farbe an. Wenn Sie eine Druckoption angeben, die der Druckertreiber nicht unterstützt, hat die Option keine Auswirkung. Mit dieser Einstellung werden die gespeicherten Druckereinstellungen überschrieben, die der Benutzer in einer vorherigen Sitzung festgelegt hat.
5. Citrix empfiehlt, das Verhalten der Drucker nach der Zuordnung von Treibern ausführlich zu testen, da einige Druckfunktionen möglicherweise nur über einen bestimmten Treiber zur Verfügung stehen.

Bei der Benutzeranmeldung wird die Clientdruckerkompatibilitätsliste vom System überprüft, bevor die Clientdrucker eingerichtet werden.

## Optimieren der Druckleistung

Verwenden Sie den universellen Druckserver und den universellen Druckertreiber, um die Leistung zu optimieren. Die folgenden Richtlinien steuern die Druckoptimierung und Komprimierung:

- Universelles Drucken - Optimierungsstandards. Gibt die Standardeinstellungen für den universellen Drucker an, wenn er für eine Sitzung erstellt wird:
  - Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
  - Mit Heavyweight-Komprimierung aktivieren aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von "Gewünschte Bildqualität" festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
  - Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert.
  - Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht ändern.
- Universelles Drucken - Bildkomprimierungslimit. Definiert die maximale Qualität und die minimale Komprimierung für Bilder, die mit dem universellen Druckertreiber gedruckt werden. Das Limit für Bildkomprimierung ist standardmäßig auf Beste Qualität (verlustfreie Komprimierung) gesetzt.
- Universelles Drucken - Druckqualitätslimit. Der Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung. In der Standardeinstellung ist kein Limit angegeben.

Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. Erwägen Sie, Druckaufträge über die ICA-Verbindung zu leiten, wenn das Netzwerk hohe Latenz oder beschränkte Bandbreite aufweist. Deaktivieren Sie hierzu die Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern. Bei einer ICA-Verbindung werden die Daten komprimiert gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

**Verbessern der Sitzungsleistung durch Limitierung der Druckbandbreite**: Beim Drucken von Dateien von Serverbetriebssystemmaschinen auf Benutzerdruckern, können bei anderen virtuellen Kanälen (z. B. Video) aufgrund des Wettbewerbs um die Bandbreite Leistungsverringerungen entstehen, insbesondere dann, wenn Benutzer über langsamere Netze auf Server zugreifen. Um dies zu verhindern, können Sie die für das Drucken verwendete Bandbreite beschränken. Indem Sie die Datenübertragungsrate für den Druck einschränken, stellen Sie im HDX-Datenstrom eine größere Bandbreite

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

für die Übertragung von Video, Tastatureingaben und Mausdaten zur Verfügung.

Wichtig: Das Druckerbandbreitenlimit wird immer eingehalten, auch wenn keine anderen Kanäle verwendet werden. Verwenden Sie die nachfolgenden Einstellungen der Citrix Richtlinie Bandbreite, um die Druckerbandbreitenlimits für die Sitzung zu beschränken. Führen Sie diese Aufgabe mit Studio aus, um die Limits für die Site festzulegen. Wenn Sie Limits für einzelne Server festlegen möchten, führen Sie diese Aufgabe über die Gruppenrichtlinien-Verwaltungskonsole in Windows lokal auf jeder Serverbetriebssystemmaschine aus.

- Die Einstellung Bandbreitenlimit für Druckerumleitung dient zur Angabe der zum Drucken verfügbaren Bandbreite in Kilobits pro Sekunde (KBit/s).
- Die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) begrenzt die zum Drucken verfügbare Bandbreite auf einen Prozentanteil der insgesamt verfügbaren Bandbreite.
  Hinweis: Zur Verwendung der Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt aktivieren.
  Wenn Sie Werte für beide Einstellungen eingeben, wird die strengste Einstellung (mit dem niedrigeren Wert) angewendet.

Zum Abrufen von Echtzeitinformationen zur Druckbandbreite verwenden Sie Citrix Director.

### Lastausgleich bei universellen Druckservern

Die universelle Druckserverlösung kann skaliert werden, indem Sie der Lastausgleichslösung weitere Druckserver hinzufügen. Es gibt keine einzelne Fehlerquelle, da jeder VDA seinen eigenen Load Balancer hat, um die Drucklast auf alle Druckserver zu verteilen.

Verwenden Sie die Richtlinieneinstellungen Universelle Druckserver für den Lastausgleich und Außer-Betrieb-Schwellenwert für universelle Druckserver, um die Drucklast in einer Lastausgleichslösung auf alle Druckserver zu verteilen.

Wenn ein Druckerserver unvorhergesehen ausfällt, werden die Druckerverbindungen des ausgefallenen Druckservers durch den Failovermechanismus des Load Balancers eines VDAs automatisch auf die anderen verfügbaren Druckerserver verteilt, sodass alle vorhandenen und eingehenden Sitzungen normal funktionieren, ohne dass die Benutzererfahrung betroffen oder ein Eingreifen des Administrators nötig ist.

Administratoren können die Aktivitäten der Lastausgleichsdruckserver mit einer Reihe von Leistungsindikatoren überwachen und Folgendes auf dem VDA verfolgen:

- Liste der Lastausgleichsdruckserver auf dem VDA und deren Zustand (verfügbar, nicht verfügbar)
- Anzahl der akzeptierten Druckerverbindungen pro Druckserver
- Anzahl der fehlgeschlagenen Druckerverbindungen pro Druckserver
- Anzahl der aktiven Druckerverbindung pro Druckserver
- Anzahl ausstehender Druckerverbindungen pro Druckserver

### Anzeigen und Verwalten der Druckwarteschlangen

In der folgenden Tabelle wird aufgeführt, wo Sie in Ihrer Umgebung Drucker anzeigen und die Druckwarteschlangen verwalten können.

| | **Druckmodell** | **UAC aktiviert?** | **Speicherort** |
|---|---|---|---|
| Clientdrucker (an das Benutzergerät angeschlossene Drucker) | Clientdruckmodell | On | Druckverwaltung: Snap-in der Microsoft |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | Druckmodell | UAC aktiviert? | Speicherort |
|---|---|---|---|
| | | Off | Vor Windows 8: Systemsteuerung Windows 8: Snap-in Druckverwaltung |
| Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver) | Netzwerkdruckmodell | On | Druckserver > Druckverwaltung Snap-in der Microsoft Management Console |
| | | Off | Druckserver > Systemsteuerung |
| Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver) | Clientdruckmodell | On | Druckserver > Druckverwaltung Snap-in der Microsoft Management Console |
| | | Off | Vor Windows 8: Systemsteuerung Windows 8: Snap-in Druckverwaltung |
| Lokale Netzwerkserverdrucker (Drucker von einem Netzwerkdruckserver, die einer Serverbetriebssystemmaschine hinzugefügt werden) | Netzwerkdruckmodell | On | Druckserver > Systemsteuerung |
| | | Off | Druckserver > Systemsteuerung |

Hinweis: Druckwarteschlangen für Netzwerkdrucker, die das Netzwerkdruckmodell verwenden, sind privat und können nicht über das System verwaltet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# HDX

Jul 08, 2016

Citrix HDX enthält eine breite Palette an Technologien für eine High-Definition-Benutzererfahrung.

| | |
|---|---|
| Auf dem Gerät | HDX nutzt die Computingfähigkeiten der Benutzergeräte und verbessert und optimiert die Benutzererfahrung. Die HDX MediaStream-Technologie liefert eine gleichmäßigen, nahtlosen Multimediainhalt in den virtuellen Desktops oder Anwendungen der Benutzer. Mit Workspace Control können Benutzer virtuelle Desktops und Anwendungen anhalten und auf einem anderen Gerät an derselben Stelle weiterarbeiten. |
| Im Netzwerk | HDX enthält erweiterte Optimierungs- und Beschleunigungsfunktionen und gewährleistet die beste Leistung in jedem Netzwerk, auch bei Verbindungen mit niedriger Bandbreite und bei WAN-Verbindungen mit hoher Latenz.<br><br>HDX-Features passen sich den Änderungen in der Umgebung an und stimmen Lastausgleich und Bandbreite anhand optimaler Technologien für die jeweiligen Benutzerszenarios aufeinander ab, und zwar sowohl bei lokalem Zugriff auf die Desktops oder Anwendungen im Unternehmensnetzwerk als auch bei Remotezugriff von außerhalb des Unternehmens. |
| Im Datencenter | HDX nutzt die Verarbeitungsleistung und die Skalierbarkeit von Servern für eine erweitere Grafikleistung, unabhängig von den Funktionen des Clientgeräts. Komprimierte Multimediainformationen werden direkt im ursprünglichen Format an das Benutzergerät gesendet.<br><br>Die in Citrix Director bereitgestellte HDX-Kanalüberwachung zeigt den Status der verbundenen HDX-Kanäle auf Benutzergeräten an.<br><br>HDX Insight, die Integration von Netzwerkinspektion und Leistungsverwaltung mit Director, erfasst Daten zum ICA-Datenverkehr und bietet eine Dashboardansicht von Echtzeit- und historischen Daten, wie die clientseitige und serverseitige ICA-Sitzungslatenz, die Bandbreitennutzung der ICA-Kanäle und die ICA-Roundtrip-Zeit für jede Sitzung. |

Erleben von HDX-Funktionen mit Ihrem virtuellen Desktop:

- Sehen Sie selbst, wie hochwertige Videoinhalte auf virtuellen Desktops mit HDX wiedergegeben werden: Zeigen Sie ein Video auf einer Website mit HD-Videos an, z. B. http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.
- Erleben Sie, wie die Flash-Umleitung die Bereitstellung von Flash-Multimediainhalten beschleunigt:
  1. Laden Sie Adobe Flash Player herunter (http://get.adobe.com/flashplayer/) und installieren Sie ihn auf dem virtuellen Desktop und dem Benutzergerät.
  2. Klicken Sie auf der Desktop Viewer-Symbolleiste auf Einstellungen. Klicken Sie im Dialogfeld Desktop Viewer-Einstellungen auf die Registerkarte Flash und wählen Sie Inhalt optimieren.
  3. Erleben Sie, wie die Flash-Umleitung die Bereitstellung von Flash-Multimediainhalten auf virtuellen Desktops beschleunigt und zeigen Sie auf dem Desktop ein Video von einer Website mit Flash-Videos an, z. B. YouTube. Die Flash-Umleitung wird nahtlos integriert, sodass Benutzer nicht wissen, wann die Software ausgeführt wird. Sie können überprüfen, ob die Flash-Umleitung ausgeführt wird, indem Sie nach einem Farbblock Ausschau halten, der vorübergehend vor dem Start von Flash Player angezeigt wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- So stellt HDX HD-Audio bereit:
  1. Konfigurieren Sie den Citrix Client für maximale Audioqualität; weitere Informationen hierzu finden Sie in der Citrix Receiver-Dokumentation.
  2. Geben Sie Musikdateien mit einem digitalen Audioplayer (z. B. iTunes) auf dem Desktop wieder.

HDX bietet standardmäßig qualitativ hochwertige Grafiken und Videos, sodass für die meisten Benutzer keine Konfiguration erforderlich ist. Die standardmäßig aktivierten Citrix Richtlinieneinstellungen liefern die beste Sofortlösung für die Mehrheit der Fälle.

- HDX wählt automatisch die beste Bereitstellungsmethode basierend auf Client, Plattform, Anwendung und Bandbreite und nimmt dann selbständig entsprechend der geänderten Bedingungen eine Einstellung vor.
- HDX optimiert die Leistung von 2D- und 3D-Grafiken und Video.
- HDX liefert den Windows-Desktopbenutzern eine Windows Aero-Oberfläche auf jedem Client.
- HDX ermöglicht das Streamen von Multimediadateien für die Benutzergeräte direkt vom Quellenanbieter im Internet oder Intranet, ohne dass der Hostserver beteiligt wird. Wenn die Anforderungen für diesen clientseitigen Inhaltsabruf nicht erfüllt sind, erfolgt die Medienbereitstellung automatisch über Windows Media-Umleitung zur Wiedergabe von Medieninhalten auf dem Benutzergerät statt auf dem Hostserver. In den meisten Fällen ist keine Änderung der Richtlinien für Windows Media erforderlich.

Gut zu wissen:

- Informationen zum Support und zu Systemanforderungen für HDX-Features finden Sie im Artikel Systemanforderungen. Sofern nicht anders angegeben, stehen HDX-Features für unterstützte Windows-Serverbetriebssystemmaschinen, Windows-Desktopbetriebssystemmaschinen und Remote-PC-Zugriff-Desktops zur Verfügung.
- Nachfolgend wird beschrieben, wie Sie die Benutzererfahrung weiter optimieren, die Skalierbarkeit verbessern oder die Bandbreitenanforderungen reduzieren können. Weitere Informationen zum Arbeiten mit Citrix Richtlinien und Richtlinieneinstellungen finden Sie unter
  *— Citrix Richtlinien*
  zu diesem Release.
- Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

## Reduzieren der Bandbreite für Windows-Desktops

HDX bietet standardmäßig eine hochgradig dynamische Windows Aero- oder Windows 8-Desktopdarstellung auf virtuellen Desktops von unterstützten Windows-Benutzergeräten. Um dies zu gewährleisten, nutzt HDX den Grafikprozessor (GPU) oder den integrierten Grafikprozessor (IGP) auf den Benutzergeräten für lokale DirectX Grafikwiedergabe. Dieses Feature wird als Desktopgestaltungsumleitung bezeichnet und gewährleistet hohe Skalierbarkeit auf dem Server. Weitere Informationen finden Sie unter "What to do with all these choices" unter http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/.

Um die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, sollten Sie die folgenden Richtlinieneinstellungen ändern. Beachten Sie, dass sich die Änderung der Einstellungen auf die Qualität der Benutzererfahrung auswirken kann.

- **Desktopgestaltungsumleitung**: Gilt nur für Windows-Desktopbetriebsystemmaschinen, auf die über Windows-Benutzergeräte zugegriffen wird und nur für die Komposition des Windows-Desktops. Anwendungsfenster werden auf dem Server wiedergegeben, es sei denn, die Citrix Richtlinieneinstellung Zugriff auf lokale Anwendungen zulassen ist zugelassen.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- **Grafikqualität Desktopgestaltungsumleitung**: Verwendet hochwertige Grafiken für die Desktopgestaltung, es sei denn, Seamless-Anwendungen oder Zugriff auf lokale Anwendungen sind aktiviert. Reduzieren Sie die Grafikqualität, um die Bandbreite zu reduzieren.
- **Dynamische Fenstervorschau**: Steuert die Anzeige von Seamlessfenstern in Flip, Flip 3D, Taskleistenvorschau und Peek-Fenstervorschau. Zum Reduzieren der Bandbreite deaktivieren Sie diese Richtlinieneinstellung.

### Verbessern der Bildqualität an Benutzergeräten

Die folgenden Richtlinieneinstellungen für "Visuelle Anzeige" steuern die Qualität der Bilder, die von virtuellen Desktops auf Benutzergeräte gesendet werden.

- Bildqualität: steuert die visuelle Qualität der Bilder auf dem Benutzergerät: Mittel, Hoch, Immer verlustfrei, Zu verlustfrei verbessern (Standardeinstellung = Mittel).
- Frameratesollwert: gibt die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden (Standardwert = 30). In vielen Fällen können Sie die Benutzererfahrung verbessern, indem Sie einen höheren Wert festlegen. Bei Geräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung.
- Anzeigespeicherlimit: gibt die maximale Größe des Videopuffers (in Kilobyte) für die Sitzung an (Standardwert = 65536 KB). Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Sie können den maximal erforderlichen Speicher berechnen. Andere Farbtiefen als 32 Bit sind nur verfügbar, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

### Verbessern der Videokonferenzleistung

Die HDX-Webcam-Videokomprimierung verbessert die Bandbreiteneffizienz und Latenztoleranz für Webcams während Videokonferenzen in einer Sitzung. Mit dieser Technologie werden die Webcamdaten über einen dedizierten virtuellen Multimediakanal gestreamt. Dies beansprucht erheblich weniger Bandbreite im Vergleich zum isochronen HDX-Plug-n-Play und funktioniert gut über WAN-Verbindungen.

Citrix Receiver-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter Mikrofon & Webcam die Einstellung Mikrofon und Webcam nicht verwenden auswählen. Um zu verhindern, dass Benutzer die HDX-Webcam-Videokomprimierung ändern, deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter "ICA > USB-Geräte".

Die HDX-Videokomprimierung ist bei Citrix Receiver unter Windows standardmäßig aktiviert, muss jedoch für Citrix Receiver unter Linux konfiguriert werden. Weitere Informationen finden Sie in der Citrix Receiver-Dokumentation. HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Clientaudioumleitung
- Clientmikrofonumleitung
- Multimediakonferenzen
- Windows Media-Umleitung

Bei Webcams, die H.264-Hardwarecodierung unterstützen, verwendet HDX-Videokomprimierung die Hardwarecodierung standardmäßig. Die Hardware-Codierung beansprucht zusätzliche Bandbreite und ist nicht für Netzwerke mit geringer Bandbreite geeignet. Zum Erzwingen der Softwarekomprimierung bei Netzwerken mit geringer Bandbreite fügen Sie den folgenden DWORD-Schlüsselwert dem Registrierungsschlüssel hinzu: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

### Bevorzugen der Skalierbarkeit des Servers vor der Benutzererfahrung

Bei Bereitstellungen, bei denen die Skalierbarkeit des Servers wichtiger ist als die Benutzererfahrung, können Sie das


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Legacygrafiksystem verwenden, indem Sie die Richtlinieneinstellung Legacygrafikmodus hinzufügen und die einzelnen Richtlinieneinstellungen für Legacygrafiken konfigurieren. Ältere Grafiksysteme wirken sich auf die Benutzererfahrung über WAN- und mobile Verbindungen aus.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Thinwire-Kompatibilitätsmodus

Jul 08, 2016

Durch neue Techniken bei der Bildschirmanalyse und -zwischenspeicherung gewährleistet der ThinWire-Kompatibilitätsmodus niedrige Bandbreitenauslastung und hohe Serverskalierbarkeit, ohne die Benutzererfahrung zu beeinträchtigen.

Der ThinWire-Kompatibilitätsmodus umfasst die folgenden Features:

- Intelligente Bitmapzuordnung für Anbieter von Bitmaps.
  - Bitmap-Übersetzungsanalyse ermöglicht effizientes Verschieben der Fenster und gleichmäßigen Bildlauf.
- Abwärtskompatibilität. Upgrades von Client oder Citrix Receiver oder Hardwarebeschleunigung sind nicht erforderlich.
  - Getestet mit zahlreichen älteren Thin Clients, bis zu 5 Jahren alt und älter.
- Optimiert für sehr niedrige Server-CPU-Auslastung und verbesserte Serverskalierbarkeit.
- Ein emulierter 16-Bit-Modus reduziert die Bandbreite um weitere 15-20 % bei typischen Arbeitslasten.
- Übergangserkennung für serverseitige Wiedergabe von Videoinhalt.
  - Verarbeitung mehrerer Übergangsbereiche für eine bessere Multimediaerfahrung. Beispiel: Wiedergabe mehrerer Videos oder Liveticker.
  - Selektives Scharfzeichnen für Bereiche, die einen Übergangszustand verlassen.
- Optimiert für CloudBridge-Beschleunigung. Tests ergaben eine Verringerung der Bandbreite im Verhältnis 6:1 bei Büroarbeitslasten.
- Adaptive Anzeige, die über Richtlinieneinstellungen angepasst werden kann. Weitere Informationen finden Sie unter **Bewegtbildkomprimierung** in Einstellungen der Richtlinie "Bewegtbilder".
- VDAs und Windows-Betriebssysteme bis zu Windows 10 VDA werden unterstützt.
- Der neue Modus "Zu verlustfrei verbessern" für 3D Pro erhöht die Reaktion, Interaktivität und unterbrechbares Scharfzeichnen für eine bessere Benutzererfahrung bei niedriger Bandbreite.
- Die Standardqualität statischer fotografischer Bilder ist höher als im Legacygrafikmodus.

Zur Steigerung der Clientleistung und Senkung der Bandbreitenauslastung werden für die Bildqualitätseinstellungen "Niedrig", "Mittel" (Standard) und "Hoch" Bildschirmaktualisierungen von der Übergangserkennung dynamisch ausgewertet, um zu entscheiden, ob hoch animierte Bereiche entsprechend der Richtlinie für die adaptive Anzeige mit niedrigerer Qualität gesendet werden.

Für die Bildqualität **Zu verlustfrei verbessern** verwendet der ThinWire-Kompatibilitätsmodus bei großen Bildschirmaktualisierungen das Prinzip "zunächst unscharf". Diese Einstellung ist für 3D Pro-Benutzer gedacht, die mit 3D-Modellen oder anderen grafikintensiven Anwendungen arbeiten. Wird die Aktivität fortgesetzt, wird ein Übergangsmodus angenommen und nach dessen Ende wird der betroffene Bereich scharfgezeichnet und zwischengespeichert. Bei der anfänglichen großen Änderung findet eine oberflächliche Bildanalyse am Änderungsbereich statt, um festzustellen, ob es sich um einen unscharfen Übergang oder um einen scharfen (verlustfreien) Übergang handelt, z. B. beim Drehen eines Drahtmodells. In puncto Framerate und Bandbreite ist die Codierung einfacher Bilder mit dem verlustfreien Citrix Codec effizienter, wobei kein Qualitätsverlust entsteht.

Der Schritt beim Scharfzeichnen bei der Einstellung "Zu verlustfrei verbessern" ist ebenfalls anders. Der Bereich wird nicht auf einmal scharfgezeichnet, sondern in vorgegebenen Blöcken für eine gleichmäßige und interaktive Benutzererfahrung. Das Scharfzeichnen eines großen Änderungsbereichs mitten im Übergang (z. B. beim Verschieben eines 3D-Modells, das kurzzeitig angehalten und dann fortgesetzt wird) würde insbesondere bei Verbindungen mit geringer Bandbreite einen Stillstand verursachen. Die Größe der Blöcke beim Scharfzeichnen hängt davon ab, wie stark die Qualität reduziert wurde,


© 1999-2017 Citrix Systems, Inc. All rights reserved.

um die Mindestframerate (eine Richtlinieneinstellung für die adaptive Anzeige) zu erzielen. Wurde die Qualität stark reduziert, sind die Blöcke beim Scharfzeichnen kleiner, die Mindestgröße beträgt 128 x 128 Pixel. Wurde die Qualität nicht reduziert, z. B. wenn der Client über ausreichend Rechenleistung und Bandbreite verfügt, können beim Scharfzeichnen Blöcke der Maximalgröße von 384 x 384 Pixel verwendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Framehawk Virtual Channel

Jul 08, 2016

# Einführung

Der virtuelle Framehawk-Kanal optimiert die Bereitstellung virtueller Desktops und Anwendungen für Benutzer über drahtlose Breitbandverbindungen und verlustbehaftete Breitbandnetzwerkverbindungen über große Distanzen mit hohem Paketverlust oder Engpässen. Sie können mit Citrix Richtlinien Framehawk oder ThinWire für Benutzergruppen in einer Weise implementieren, die den gegebenen Netzwerkeigenschaften angepasst ist und den allgemeinen Erwartungen an Skalierbarkeit und Leistung entspricht.

Bisher galten generell Framerate und Anzeigequalität als Basisparameter für eine positive Benutzererfahrung. Durch Framehawk wird diese Definition um den Begriff der Linearität erweitert. Die Benutzer sollten ohne Ablenkung in den Genuss einer guten Benutzererfahrung kommen. In einem problembehafteten Netzwerk tritt der bei allen Protokollen bekannte Gummibandeffekt auf. Dieser verleitet den Benutzer, der nicht sicher ist, ob der Bildschirm noch reagiert, zu erratischen Mausklicks und führt zu unerwünschten Ergebnissen. Framehawk vermindert dieses Problem, insbesondere bei schwierigen Netzwerkbedingungen.

Bei privaten High-Speed-Internet-Verbindungen treten häufig Leistungsprobleme auf, z. B. aufgrund von Konflikten mit benachbarten WiFi-Signalen oder Funkstörungen, die durch schnurlose Geräte verursacht werden. Immer mehr Benutzer stellen eine Verbindung mit gehosteten Apps und Daten über 3G- oder 4G/LTE-Mobilfunknetze her oder verwenden Inflight-Internet-Dienste. Beliebt sind auch öffentliche WLAN-Hotspots in Cafés und Hotels, wo ebenfalls häufig Netzwerkengpässe auftreten.

Mit Framehawk wird die Benutzererfahrung bei hoher Latenz interaktiver (stärker lineares Echoback der Zeichen).

## Wirkungsweise von Framehawk

Bei der Betrachtung des Inhalts des Framepuffers und der Unterscheidung verschiedener Inhaltsarten auf dem Bildschirm wirkt Framehawk wie das menschliche Auge. Was ist dem Benutzer wichtig? In Bildschirmbereichen mit schnellen Änderungen (Video, Animationen etc.) spielt es für das menschliche Auge keine Rolle, wenn einige Pixel verloren gehen, da sie schnell durch neue Daten überschrieben werden.

Bei statischen Bereichen, z. B. Symbolleisten oder Text kurz nach Ausführen eines Bildlaufs an, den der Benutzer direkt lesen möchte, ist das menschliche Auge sehr anspruchsvoll. Diese Bereiche müssen pixelgenau sein. Im Gegensatz zu Protokollen, bei denen dich technische Präzision im Sinne von Nullen und Einsen im Vordergrund steht, ist Framehawk stärker auf die menschlichen Nutzer von Technik ausgelegt.

Framehawk umfasst einen völlig neuen QoS-Signalverstärker sowie eine zeitabhängige Heatmap zur exakteren und effizienten Arbeitslasterkennung. Zusätzlich zur Datenkomprimierung werden in Framehawk autonome, selbstkorrigierende Transformationen verwendet, die erneute Übertragung von Daten wird zur Gewährleistung von Klickantwort, Linearität und konsistenter Kadenz vermieden. In einem verlustreichen Netzwerk kann Framehawk Verluste durch Interpolation ausgleichen, sodass der Benutzer die Bildqualität weiterhin als gut empfindet und die Benutzererfahrung sogar flüssiger wird. Die Algorithmen von Framehawk können darüber hinaus die verschiedenen Arten des Paketverlusts unterscheiden, etwa den regellosen Verlust (weitere Daten zur Kompensierung senden) und den Verlust durch Engpässe (keine weiteren Daten senden, da der Kanal bereits blockiert ist).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Framehawk Intent Engine unterscheidet Bildlauf nach oben oder unten, Vergrößern, Verschieben nach links oder rechts, Lesen, Eingeben und weitere übliche Aktionen und steuert die Antwort an den Virtual Delivery Agent (VDA) mit einem freigegebenen Wörterbuch. Wenn der Benutzer lesen möchte, muss die visuelle Qualität des Texts hervorragend sein. Führt er einen Bildlauf durch, muss dieser schnell und gleichmäßig sein. Er muss außerdem unterbrochen werden können, damit der Benutzer die Interaktion mit der Anwendung oder dem Desktop jederzeit unter Kontrolle hat.

Durch die Messung der Kadenz der Netzwerkverbindung kann die Framehawk-Logik schneller reagieren und bei Verbindungen mit hoher Latenz eine bessere Benutzererfahrung ermöglichen. Dieses einzigartige, patentierte Verfahren liefert kontinuierlich aktuelle Rückmeldungen zu Netzwerkbedingungen, sodass Framehawk auf Änderungen bei Bandbreite, Latenz und Verlust sofort reagieren kann.

# ThinWire und Framehawk – Überlegungen zur Auslegung

ThinWire ist branchenweit erste Wahl in puncto Bandbreiteneffizienz und eignet sich gut für viele Zugriffsszenarien und Netzwerkbedingungen. Allerdings wird zur Gewährleistung einer zuverlässigen Datenkommunikation bei ThinWire TCP verwendet, wodurch in verlustreichen oder überlasteten Netzwerken eine Paketneuübertragung erforderlich ist, um Verzögerungen beim Endbenutzer zu vermeiden.

Die Datenübertragung bei Framehawk basiert auf UDP und damit auf dem Ansatz "so gut wie möglich". UDP macht nur einen kleinen Teil der Überwindung von Paketverlusten bei Framehawk aus, was deutlich wird, wenn man seine Leistung mit der anderer UDP-basierter Protokolle vergleicht. Allerdings bildet UDP die Grundlage für die menschenorientierte Technik, die Framehawk von anderen Lösungen abhebt.

Wie viel Bandbreite benötigt Framehawk?

Die Bezeichnung Breitband-WLAN hängt von verschiedenen Faktoren ab, etwa der Zahl der Benutzer, die eine Verbindung teilen, der Qualität der Verbindung und der verwendeten Apps. Zur Erzielung einer optimalen Leistung empfiehlt Citrix einen Grundwert von 4 oder 5 MBit/s plus ca. 150 KBit/s pro gleichzeitig verbundenem Benutzer.

Citrix empfiehlt für ThinWire generell eine Bandbreite von 1,5 MBit/s plus 150 KBit/s pro Benutzer (Details siehe Blog zu XenApp- und XenDesktop-Bandbreite), bei einem Paketverlust von 3 % benötigt ThinWire aber viel mehr Bandbreite als Framehawk, um eine gute Benutzererfahrung zu gewährleisten.

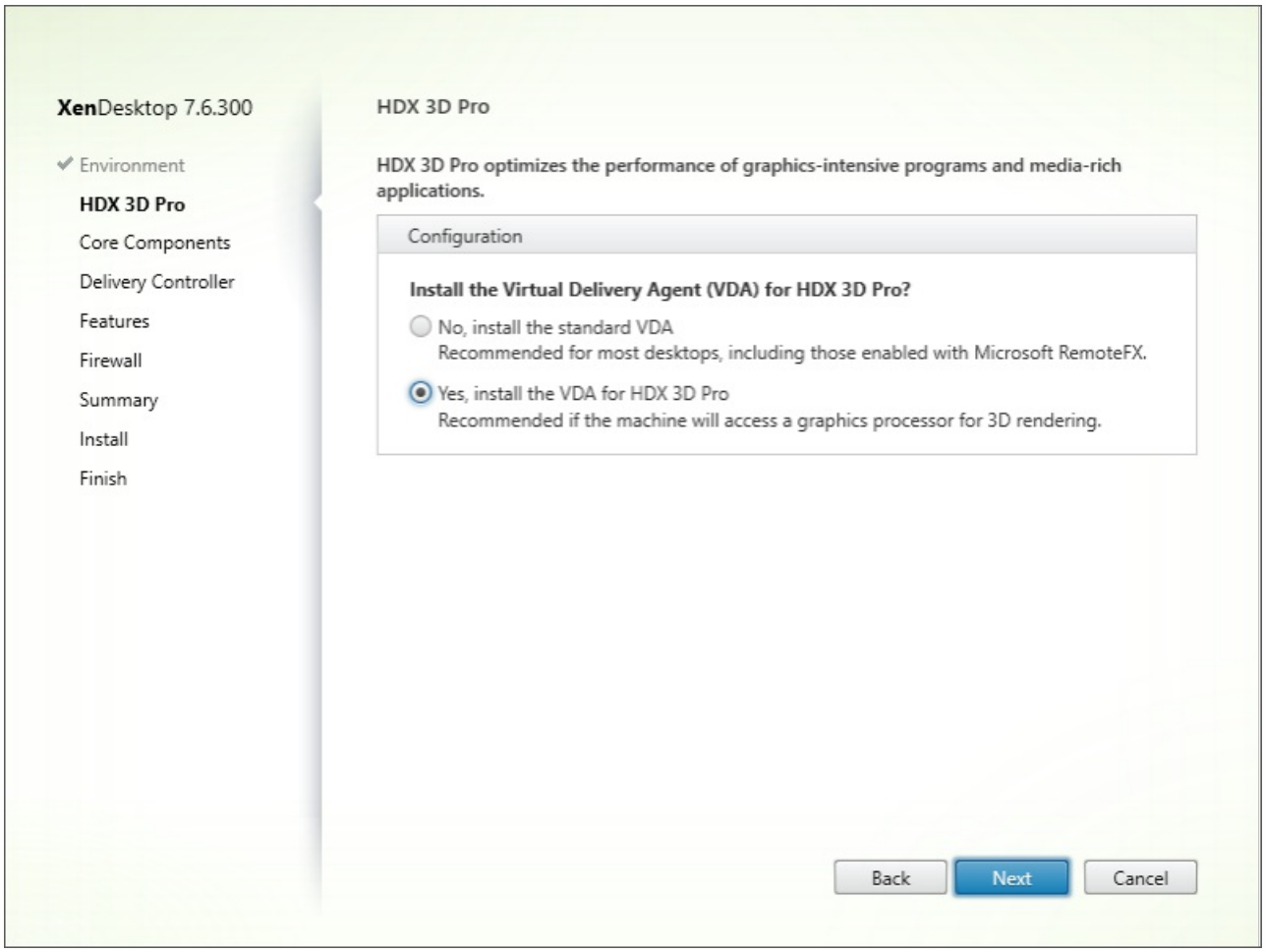
Hinweis: ThinWire ist weiterhin der Primärkanal für das Anzeigen-Remoting des ICA-Protokolls. Framehawk ist standardmäßig deaktiviert. Citrix empfiehlt die selektive Aktivierung für spezifische Breitband-WLAN-Szenarios in Ihrer Organisation.

## Framehawk und HDX 3D Pro

Framehawk unterstützt jetzt alle Anwendungsfälle von HDX 3D Pro für XenApp-Apps (Serverbetriebssystem) und XenDesktop-Apps (Desktopbetriebssystem). In frühen Previews wurden in Kundenumgebungen Latenzen von 400-500 ms und Paketverluste von 1-2 % gemessen, wodurch bei gebräuchlichen Anwendungen zur 3D-Modellierung (z. B. AutoCAD, Siemens NX) eine gute Interaktivität erzielt wird. Diese Unterstützung ermöglicht nun auch die Anzeige von und Arbeit an großen CAD-Modellen im mobilen Einsatz oder an entfernten Standorten mit schlechten Netzwerkverbindungen.

Zur Aktivierung dieser Funktion ist keine gesonderte Konfiguration erforderlich. Beim Installieren des VDAs wählen Sie die 3DPro-Option zu Beginn der Installation aus:

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 




# Anforderungen und Überlegungen

Framehawk erfordert mindestens VDA 7.6.300 und Gruppenrichtlinienverwaltung 7.6.300.

Auf dem Endpunkt muss mindestens Citrix Receiver für Windows 4.3.100 oder Citrix Receiver für iOS 6.0.1 ausgeführt werden.

Standardmäßig verwendet Framehawk den bidirektionalen UDP-Portbereich (3224-3324) zum Austausch von Framehawk-Anzeigekanaldaten mit Citrix Receiver. Dieser Bereich kann über die Richtlinieneinstellung "Portbereich für Framehawk-Anzeigekanal" angepasst werden. Jede einzelne Verbindung zwischen dem Client und dem virtuellen Desktop erfordert einen eigenen Port. In Betriebssystemumgebungen mit mehreren Benutzern (z. B. XenApp-Server) müssen Sie ausreichend Ports für die maximale Zahl gleichzeitiger Benutzersitzungen definieren. Bei Einzelbenutzer-Betriebssystemen wie etwa VDI-Desktops reicht ein UDP-Port. Framehawk versucht die Verwendung der Ports beginnend vom ersten bis zum letzten im angegebenen Bereich. Dies gilt sowohl für Verbindungen über NetScaler Gateway als auch für direkte interne Verbindungen mit dem StoreFront-Server.

Für den Remotezugriff muss NetScaler Gateway bereitgestellt sein. Standardmäßig verwendet NetScaler UDP-Port 443 für die verschlüsselte Kommunikation zwischen Citrix Receiver auf dem Client und dem Gateway. Dieser Port muss in allen externen Firewalls geöffnet sein, damit eine sichere Kommunikation in beide Richtungen möglich ist. Das Feature wird als "Datagram Transport Security" (DTLS) bezeichnet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Hinweis**: Framehawk-/DTLS-Verbindungen werden auf FIPS-Geräten nicht unterstützt.

Verschlüsselte Framehawk-Verbindungen werden unter NetScaler Gateway ab Version 11.0.62 und unter NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

Bei der Implementierung virtueller Framehawk-Kanäle empfehlen sich folgende bewährte Methoden:

- Vergewissern Sie sich beim Sicherheitsadministrator, dass die für Framehawk definierten UDP-Ports in der Firewall geöffnet sind. Die Firewall wird bei der Installation nicht automatisch konfiguriert.
- In vielen Fällen ist NetScaler Gateway in der DMZ umgeben von einer externen und einer internen Firewall installiert. UDP-Port 443 muss in der externen Firewall geöffnet sein. Wenn die Standardportbereiche verwendet werden, muss der UDP-Portbereich 3224-3324 in der internen Firewall geöffnet sein.

# Konfiguration

**Achtung:** Framehawk sollte nur für Benutzer mit hohem Paketverlust aktiviert werden. Es wird außerdem empfohlen, Framehawk nicht als universelle Richtlinie für alle Objekte der Site zu aktivieren.

Framehawk Virtual Channel ist standardmäßig deaktiviert. Wenn das Feature aktiviert ist, versucht der Server, Framehawk Virtual Channel für die Grafiken und Eingaben der Benutzer zu verwenden. Sind die Voraussetzungen nicht erfüllt, wird die Verbindung im Standardmodus (ThinWire) hergestellt.

Die folgenden Richtlinieneinstellungen wirken sich auf Framehawk aus:

- Framehawk-Anzeigekanal: aktiviert oder deaktiviert das Feature.
- Portbereich für Framehawk-Anzeigekanal: Bereich der UDP-Portnummern (niedrigste Portnummer bis höchste Portnummer), die der VDA für den Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

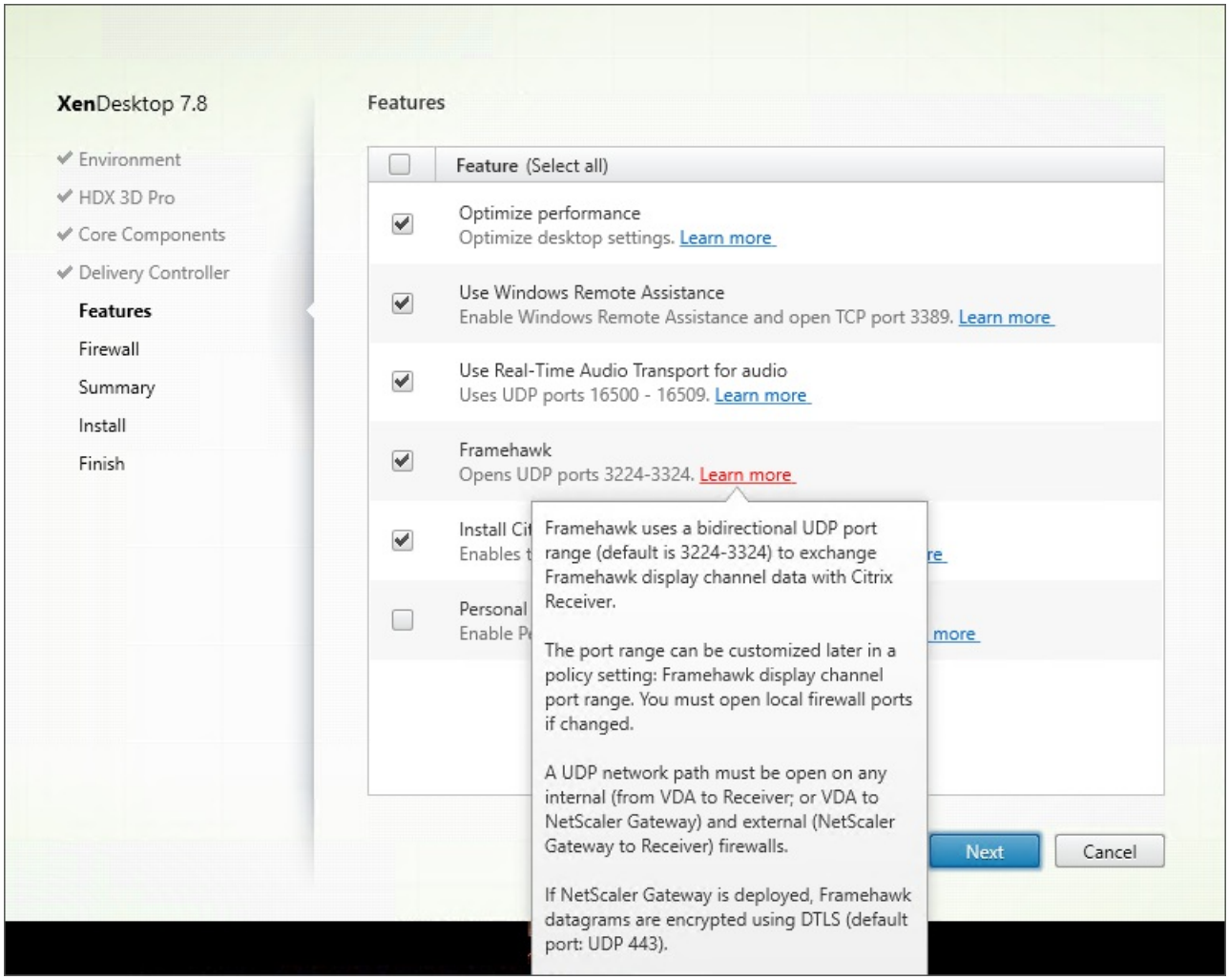
## Öffnen von Ports für den Framehawk-Anzeigekanal

In Release 7.8 gibt es eine neue Option zum Konfigurieren der Firewall im Schritt **Features** des VDA-Installationsprogramms. Über das zugehörige Kontrollkästchen werden die UDP-Ports 3224-3324 in der Windows-Firewall geöffnet. In folgenden Fällen ist eine manuelle Firewallkonfiguration erforderlich:

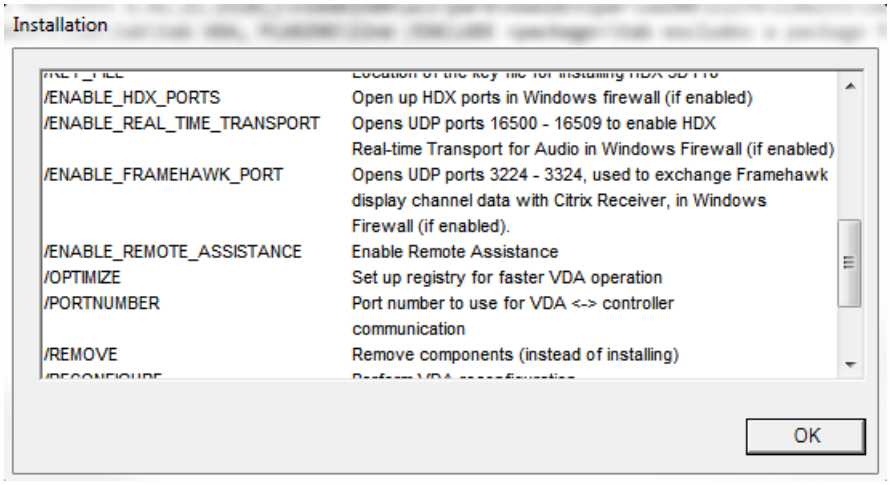
- Es handelt sich um eine Netzwerkfirewall.
- Der Standardportbereich wird angepasst.

Zum Öffnen der UDP-Ports aktivieren Sie das Kontrollkästchen **Framehawk**:


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Sie können die UDP-Ports für Framehawk Virtual Channel auch über die Befehlszeile durch Eingabe von **/ENABLE_FRAMEHAWK_PORT** öffnen:

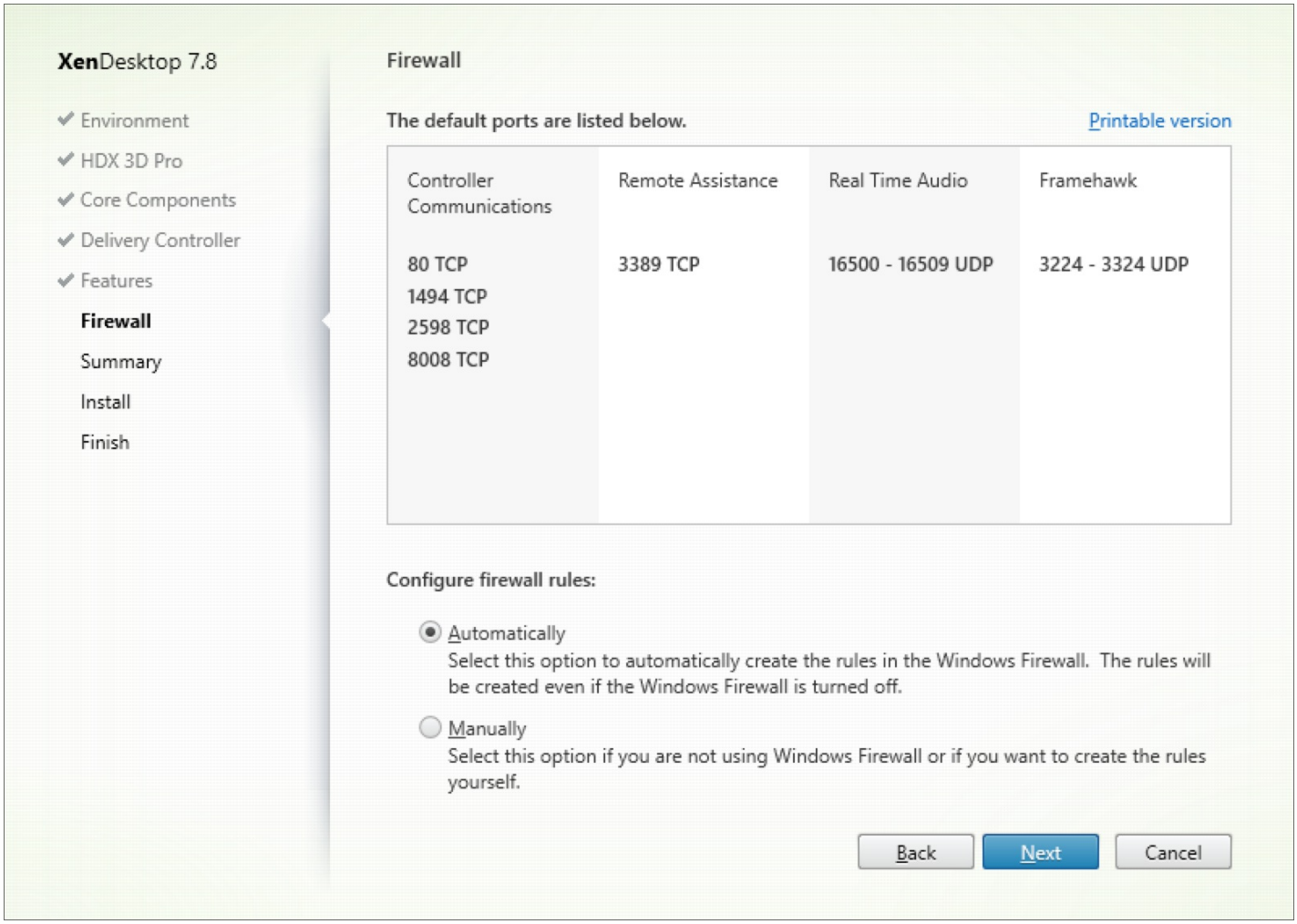



## Überprüfen der UDP-Portzuweisungen für Framehawk

Während der Installation können Sie die Framehawk Virtual Channel zugewiesenen UDP-Ports im Bildschirm **Firewall**

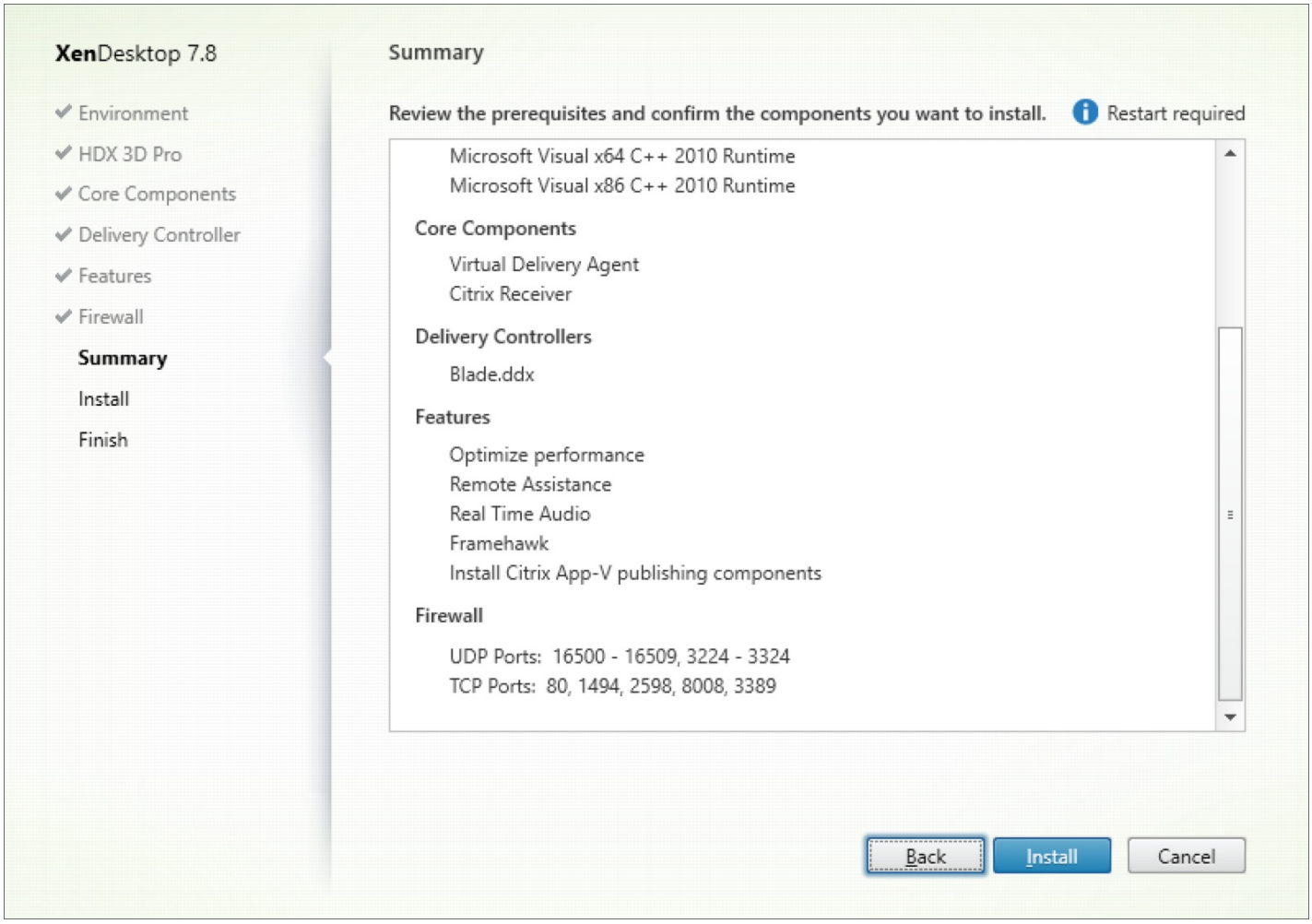

© 1999-2017 Citrix Systems, Inc. All rights reserved.

überprüfen:




Auf der Registerkarte **Zusammenfassung** wird angezeigt, ob Framehawk Virtual Channel aktiviert ist:


© 1999-2017 Citrix Systems, Inc. All rights reserved.




# NetScaler Gateway-Unterstützung für Framehawk

Verschlüsselter Framehawk-Datenverkehr wird unter NetScaler Gateway ab Version 11.0.62.10 und unter NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

- NetScaler Gateway bezieht sich auf eine Bereitstellungsarchitektur, in der der virtuelle Gateway-VPN-Server direkt für das Gerät des Endbenutzers zugänglich ist, d. h. der virtuelle VPN-Server hat eine öffentliche IP-Adresse und der Benutzer stellt direkt eine Verbindung mit dieser IP-Adresse her.
- NetScaler Unified Gateway bezieht sich auf eine Bereitstellung, in der der virtuelle Gateway-VPN-Server als Ziel an den virtuellen Content Switching-Server (CS) gebunden ist. In einer solchen Bereitstellung hat der virtuelle CS-Server die öffentliche IP-Adresse und der virtuelle Gateway-VPN-Server hat eine Pseudo-IP-Adresse.

Zum Aktivieren der Framehawk-Unterstützung unter NetScaler Gateway muss der DTLS-Parameter auf der Ebene des virtuellen Gateway-VPN-Servers aktiviert sein. Wenn der Parameter aktiviert ist und die Komponenten in XenApp bzw. XenDesktop ordnungsgemäß aktualisiert wurden, wird der Audio-, Video- und Interaktionsdatenverkehr von Framehawk zwischen dem virtuellen Gateway-VPN-Server und dem Benutzergerät verschlüsselt.

NetScaler Gateway, Unified Gateway und NetScaler Gateway + Global Server Load Balancing werden mit Framehawk unterstützt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Folgendes wird mit Framehawk nicht unterstützt:

- HDX Insight
- NetScaler Gateway im IPv6-Modus
- NetScaler Gateway Double Hop
- Mehrere Secure Ticket Authoritys (STA) für NetScaler Gateway
- NetScaler Gateway mit hoher Verfügbarkeit
- NetScaler Gateway im Cluster

| Szenario | Unterstützung für Framehawk |
|---|---|
| NetScaler Gateway | Ja |
| NetScaler + Global Server Load Balancing | Ja |
| NetScaler mit Unified Gateway | Ja<br><br>Hinweis: Unified Gateway wird ab Version 11.0.64.34 unterstützt. |
| HDX Insight | Nein |
| NetScaler Gateway im IPv6-Modus | Nein |
| NetScaler Gateway Double Hop | Nein |
| Mehrere Secure Ticket Authoritys (STA) für NetScaler Gateway | Nein |
| NetScaler Gateway mit hoher Verfügbarkeit | Nein |
| NetScaler Gateway im Cluster | Nein |

## Konfigurieren der NetScaler-Unterstützung für Framehawk

Zum Aktivieren der Framehawk-Unterstützung unter NetScaler Gateway muss der DTLS-Parameter auf der Ebene des virtuellen Gateway-VPN-Servers aktiviert sein. Wenn der Parameter aktiviert ist und die Komponenten in XenApp bzw. XenDesktop ordnungsgemäß aktualisiert wurden, wird der Audio-, Video- und Interaktionsdatenverkehr von Framehawk zwischen dem virtuellen Gateway-VPN-vServer und dem Benutzergerät verschlüsselt.

Diese Konfiguration ist erforderlich, wenn Sie die UDP-Verschlüsselung unter NetScaler Gateway für den Remotezugriff aktivieren.

NetScaler-Unterstützung für Framehawk erfordert Folgendes:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- UDP-Port 443 muss in der externen Firewall geöffnet sein.
- CGP-Standardport 2598 muss in der externen Firewall geöffnet sein.
- DTLS muss in den Einstellungen des virtuellen VPN-Servers aktiviert sein.
- Lösen Sie die Bindung des SSL-Zertifikatschlüsselpaars und binden Sie es erneut. Dies ist nicht erforderlich, wenn Sie NetScaler ab Version 11.0.64.34 verwenden.

Konfigurieren der NetScaler Gateway-Unterstützung für Framehawk

1. Stellen Sie NetScaler Gateway bereit und konfigurieren Sie es für die Kommunikation mit StoreFront und zur Authentifizierung der Benutzer von XenApp und XenDesktop.
2. Erweitern Sie auf der Registerkarte "Configuration" von NetScaler die Option "NetScaler Gateway" und wählen Sie **Virtual Servers**.
3. Klicken Sie auf **Edit**, um die Grundeinstellungen des virtuellen VPN-Servers anzuzeigen und prüfen Sie die DTLS-Einstellung.
4. Klicken Sie auf **More**, um weitere Konfigurationsoptionen aufzurufen:
5. Wählen Sie **DTLS**, um die Sicherheit für Datagramm-Protokolle wie Framehawk zu aktivieren. Klicken Sie auf **OK**. Im Bereich mit den Grundeinstellungen des virtuellen VPN-Servers wird das DTLS-Flag mit der Einstellung **True** angezeigt.
6. Öffnen Sie den Bildschirm "Server Certificate Binding" erneut und klicken Sie auf **+**, um das Zertifikatschlüsselpaar zu binden.
7. Wählen Sie das Zertifikatschlüsselpaar (s. oben) und dann **Select**.
8. Speichern Sie die Änderungen an der Serverzertifikatbindung.
9. Nach dem Speichern wird das Zertifikatschlüsselpaar angezeigt. Klicken Sie auf **Bind**.
10. Ignorieren Sie Meldung "No usable ciphers configured on the SSL vserver/service", sofern sie angezeigt wird.

## Zusätzliche Schritte bei älteren NetScaler Gateway-Versionen

Wenn Sie eine ältere Version als NetScaler Gateway 11.0.64.34 verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Bildschirm "Server Certificate Binding" erneut und klicken Sie auf +, um das Zertifikatschlüsselpaar zu binden.
2. Wählen Sie das Zertifikatschlüsselpaar (s. oben) und dann "Select".
3. Speichern Sie die Änderungen an der Serverzertifikatbindung.
4. Nach dem Speichern wird das Zertifikatschlüsselpaar angezeigt. Klicken Sie auf "Bind".
5. Ignorieren Sie Meldung "No usable ciphers configured on the SSL vserver/service", sofern sie angezeigt wird.

Konfigurieren der Unified Gateway-Unterstützung für Framehawk

1. Vergewissern Sie sich, dass Unified Gateway installiert und richtig konfiguriert ist. Weitere Informationen finden Sie auf der Website mit der Citrix Produktdokumentation unter Unified Gateway.
2. Aktivieren Sie DTLS im virtuellen VPN-Server, der an den virtuellen CS-Server als virtueller Zielserver gebunden ist.

### Unterstützung für andere VPN-Produkte

NetScaler Gateway ist das einzige SSL VPN-Produkt, das die von Framehawk benötigte UDP-Verschlüsselung unterstützt. Die Framehawk-Richtlinie wird möglicherweise nicht angewendet, wenn ein anderes SSL-VPN oder eine falsche Version von NetScaler Gateway verwendet wird. Konventionelle IPSec VPNs-Produkte unterstützen Framehawk, ohne dass eine Modifizierung erforderlich ist.

# Konfigurieren von Citrix Receiver für iOS zur


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Framehawk-Unterstützung

Zum Konfigurieren von Citrix Receiver für iOS zur Framehawk-Unterstützung müssen Sie die Datei default.ica manuell bearbeiten.

1. Öffnen Sie auf dem StoreFront-Server das App_Data-Verzeichnis im Pfad c:\inetpub\wwwroot\.
2. Öffnen Sie die Datei default.ica und fügen Sie im Abschnitt "WFClient" die Zeile "Framehawk=On" hinzu.
3. Speichern Sie die Änderung.

Damit können Framehawk-Sitzungen von kompatiblen Citrix Receiver-Instanzen auf iOS-Geräten hergestellt werden. Dieser Schritt ist nicht erforderlich, wenn Sie Citrix Receiver für Windows verwenden.

# Überwachen von Framehawk

Sie können die Verwendung und Leistung von Framehawk über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembehandlung des virtuellen Framehawk-Kanals in jeder Sitzung. Zum Anzeigen von Zahlen für Framehawk wählen Sie **Grafiken - Framehawk**.

Wenn die Framehawk-Verbindung steht, wird auf der Detailseite **Anbieter = VD3D** und **Verbunden = True** angezeigt. Der Status "Im Leerlauf" des virtuellen Kanals ist normal, da er den Signalkanal überwacht, der nur beim ersten Handshake verwendet wird. Die Seite bietet auch andere nützliche Statistiken zu der Verbindung.

Wenn Probleme auftreten, besuchen Sie das Blog zur Problembehandlung bei Framehawk.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# HDX 3D Pro

Jul 08, 2016

Mit HDX 3D Pro können Sie Desktops und Anwendungen bereitstellen, die am besten mit einem Grafikprozessor (GPU) für die Hardware-Beschleunigung arbeiten, einschließlich professioneller auf OpenGL und DirectX basierender 3D-Grafikanwendungen. Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX. Weitere Informationen zur Auswahl des Standard- oder HDX 3D Pro-VDAs finden Sie unter Angaben bei der VDA-Installation unter Vorbereiten der Installation.

Beispiele für professionelle 3D-Anwendungen:

- CAD-, CAM- und CAE-Anwendungen
- Geografische Informationssystemsoftware (GIS)
- Bildarchivierungskommunikationssystem (PACS) für bildgebende Diagnostik
- Anwendungen, die die aktuellen Versionen von OpenGL, DirectX, NVIDIA, CUDA, OpenCL und WebGL verwenden
- Rechenintensive Nichtgrafik-Anwendungen, die NVIDIA CUDA-GPUs (Compute Unified Device Architecture)für paralleles Computing verwenden

HDX 3D Pro bietet die beste bandbreitenunabhängige Benutzererfahrung:

- Für WAN-Verbindungen: Stellen Sie eine interaktive Benutzererfahrung über WAN-Verbindungen mit geringen Bandbreiten bis zu 1,5 MBit/s bereit.
- LAN-Verbindungen: Stellen Sie eine Benutzererfahrung wie bei einem lokalen Desktop bei LAN-Verbindungen mit Bandbreiten von 100 MBit/s bereit.
  Sie können komplexe und teure Arbeitsstationen durch einfache Benutzergeräte ersetzen, da die Grafikverarbeitung in das Datencenter für eine zentralisierte Verwaltung verschoben wird.

HDX 3D Pro stellt Windows-Desktopbetriebssystemmaschinen und Windows-Serverbetriebssystemmaschinen die GPU-Beschleunigung bereit. HDX 3D Pro bietet vGPU-Beschleunigung für Windows-Desktopbetriebssystemmaschinen bei Verwendung mit Citrix XenServer und NVIDIA GRID-GPUs. Informationen zu den unterstützten XenServer-Versionen finden Sie unter Citrix Virtual GPU Solution.

Mit dem HDX Monitor-Tool, dass das Tool für die Systemdiagnose ersetzt, können Sie den Betrieb und die Konfiguration von HDX-Visualisierungstechnologien überprüfen und HDX-Probleme diagnostizieren und beheben. Das Tool und weitere Informationen stehen unter https://taas.citrix.com/hdx/download zur Verfügung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Flash-Umleitung

Jul 08, 2016

Bei der Flash-Umleitung wird die Verarbeitung der meisten Adobe Flash-Inhalte (einschließlich Animationen, Videos und Anwendungen) an über LAN- und WAN-angeschlossene Windows-Benutzergeräte übertragen, wodurch Server- und Netzwerklast verringert werden. Dies führt zu größerer Skalierbarkeit, während gleichzeitig eine High Definition-Benutzererfahrung sichergestellt wird. Das Konfigurieren der Flash-Umleitung erfordert sowohl server- als auch clientseitige Einstellungen.

**Achtung:** Bei der Flash-Umleitung findet eine erhebliche Anzahl von Interaktionen zwischen dem Benutzergerät und den Serverkomponenten statt. Verwenden Sie dieses Feature nur in Umgebungen, in denen eine sicherheitsbedingte Trennung zwischen dem Benutzergerät und dem Server nicht erforderlich ist. Zudem müssen Benutzergeräte so konfiguriert werden, dass sie dieses Feature nur mit vertrauenswürdigen Servern verwenden. Da für die Flash-Umleitung der Flash Player auf dem Benutzergerät installiert sein muss, aktivieren Sie diese Funktion nur, wenn der Flash Player gesichert ist.

Die zweite Generation und Legacyversionen der Flash-Umleitung sind unabhängige Lösungen und werden in separaten virtuellen Kanälen ausgeführt.

- Legacy-Flash-Umleitungsfeatures werden nur auf dem Client unterstützt. Wenn eine ältere Version oder gar keine Version des Flash Players auf dem Benutzergerät installiert ist, werden Flash-Inhalte auf dem Server wiedergegeben.
- Die zweite Generation der Flash-Umleitung wird sowohl auf Clients als auch auf Servern unterstützt. Wenn der Client die Flash-Umleitung der zweiten Generation unterstützt, werden Flash-Inhalte auf dem Client wiedergegeben. Flash-Umleitungsfeatures der zweiten Generation bieten Unterstützung für Benutzerverbindungen über das WAN, intelligentes Fallback und eine URL-Kompatibilitätsliste. Weitere Details finden Sie weiter unten.

Flash-Umleitung verwendet die Windows-Ereignisprotokollierung auf dem Server, um Flash-Ereignisse zu protokollieren. Das Ereignisprotokoll gibt an, ob Flash-Umleitung verwendet wird und ob Probleme vorliegen. Folgendes gilt für alle Ereignisse, die von der Flash-Umleitung protokolliert werden:

- Die Flash-Umleitung meldet Ereignisse an das Anwendungsprotokoll.
- Unter Windows 8 und Windows 7 wird ein spezifisches Protokoll für die Flash-Umleitung im Knoten "Anwendungs- und Dienstprotokolle" angezeigt.
- Der Quellwert ist Flash.
- Es wird keine Kategorie angegeben.

Aktuelle Updates für HDX Flash-Kompatibilität finden Sie unter CTX136588.

## Konfigurieren der Flash-Umleitung auf dem Server

Zum Konfigurieren der Flash-Umleitung auf dem Server verwenden Sie die folgenden Citrix Richtlinieneinstellungen: Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Flash-Umleitung".

- Flash-Standardverhalten: Legt das Standardverhalten der Flash-Beschleunigung fest. Standardmäßig ist die Flash-Umleitung aktiviert. Zum Überschreiben dieses Standardverhaltens für einzelne Webseiten und Flash-Instanzen verwenden Sie die Einstellung Flash-URL-Kompatibilitätsliste.
- Flash - intelligentes Fallback:Erkennt kleinere Flash-Filme (z. B. Werbefilme) und gibt sie auf dem Server wieder statt sie zur Wiedergabe auf das Benutzergerät umzuleiten. Dies verursacht keine Unterbrechung oder Fehler beim Laden der Webseite oder der Flash-Anwendung. Standardmäßig ist "Flash - intelligentes Fallback" aktiviert. Zum Umleiten aller Flash-Inhalte für die Wiedergabe auf dem Benutzergerät deaktivieren Sie diese Richtlinieneinstellung.
- URL-Liste für serverseitigen Flash-Inhaltsabruf: Mit dieser Liste können Sie die Websites angeben, deren Flash-Inhalte zum Server heruntergeladen und dann zur Wiedergabe zum Benutzergerät gesendet werden. (Bei der standardmäßigen Flash-


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Umleitung werden Flash-Inhalte auf das Benutzergerät heruntergeladen und dort wiedergegeben.) Diese Einstellung ist zwingend mit der Einstellung Serverseitigen Inhaltsabruf aktivieren auf dem Benutzergerät verknüpft und ist hauptsächlich für Intranetsites und interne Flash-Anwendungen vorgesehen. Weitere Informationen finden Sie weiter unten. Sie funktioniert auch mit den meisten Websites und kann verwendet werden, wenn das Benutzergerät keinen direkten Internetzugang hat (z. B. wenn der XenApp- oder XenDesktop-Server die Verbindung herstellt).
Hinweis: Beim serverseitigen Inhaltsabruf werden keine Flash-Anwendungen unterstützt, die Real Time Messaging Protocol (RTMP) verwenden; stattdessen wird serverseitiges Rendering verwendet, bei dem HTTP und HTTPS unterstützt werden.

- Flash-URL-Kompatibilitätsliste: Gibt an, wo Flash-Inhalte von aufgelisteten Websites wiedergegeben werden: auf dem Benutzergerät, auf dem Server oder ob die Wiedergabe blockiert wird.
- Flash-Hintergrundfarbenliste: Hiermit können Sie die Farben von Webseiten und Flash-Instanzen aufeinander abstimmen, wodurch die Darstellung der Webseite bei Flash-Umleitung verbessert wird.

## Konfigurieren der Flash-Umleitung auf dem Benutzergerät

Installieren Sie Citrix Receiver und Adobe Flash Player auf dem Benutzergerät. Es ist keine weitere Konfiguration auf dem Benutzergerät erforderlich.

Sie können die Standardeinstellungen mit Active Directory-Gruppenrichtlinienobjekten ändern. Importieren und fügen Sie die administrative Vorlage für HDX MediaStream Flash-Umleitung - Client (HdxFlashClient.adm) hinzu, die im folgenden Verzeichnis verfügbar ist:

- 32-Bit-Computer: %Programme%\Citrix\ICA Client\Configuration\Sprache
- 64-Bit-Computer: %Programme (x86)%\Citrix\ICA Client\Configuration\Sprache

Die Einstellungen werden unter Administrative Vorlagen > Klassische administrative Vorlage (ADM) > HDX MediaStream Flash-Umleitung - Client aufgeführt. Weitere Informationen über Gruppenrichtlinienobjekten und Vorlagen finden Sie in der Dokumentation zu Microsoft Active Directory.

**Ändern der Verwendung der Flash-Umleitung**

Zusammen mit serverseitigen Einstellungen steuert die Richtlinie HDX MediaStream-Flash-Umleitung auf dem Benutzergerät, ob Adobe Flash-Inhalte für die lokale Wiedergabe auf dem Benutzergerät umgeleitet werden. Standardmäßig ist die Flash-Umleitung aktiviert und ermittelt mit der intelligenten Netzwerkerkennung, wann Flash-Inhalte auf dem Benutzergerät wiedergegeben werden.

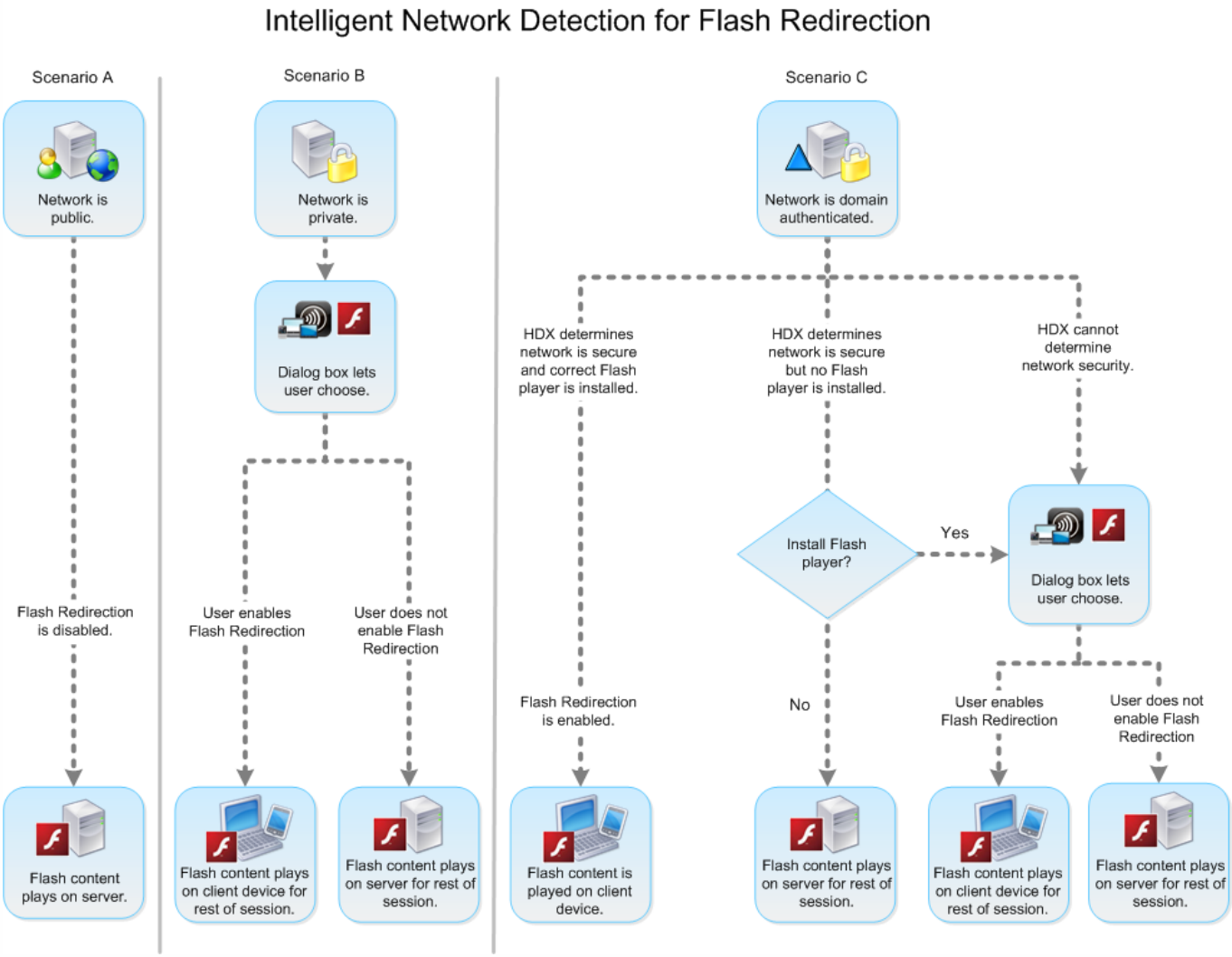
Wenn keine Konfiguration festgelegt ist und Desktop Lock verwendet wird, wird die Flash-Umleitung auf dem Benutzergerät standardmäßig aktiviert.

Gehen Sie zum Ändern der Verwendung von Flash-Umleitung bzw. zum Deaktivieren der Flash-Umleitung auf dem Benutzergerät wie folgt vor:

1. Wählen Sie aus der Einstellungsliste den Eintrag HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert (Standardeinstellung) oder Deaktiviert.
3. Wenn Sie Aktiviert eingestellt haben, wählen Sie eine Option unter HDX MediaStream Flash-Umleitung verwenden aus:
   - Die Einstellung Nur zweite Generation dient dazu, die aktuelle Flash-Umleitung zu verwenden, wenn die erforderliche Konfiguration vorhanden ist bzw. auf serverseitige Wiedergabe umzuschalten, wenn dies nicht der Fall ist.
   - Bei Wahl von Immer wird die Flash-Umleitung immer verwendet. Flash-Inhalte werden auf dem Benutzergerät wiedergegeben.
   - Bei Wahl von Nie wird die Flash-Umleitung nie verwendet. Flash-Inhalte werden auf dem Server wiedergegeben.
   - Mit Fragen (Standardeinstellung) wird festgelegt, dass die Entscheidung, ob Flash-Umleitung verwendet wird, durch

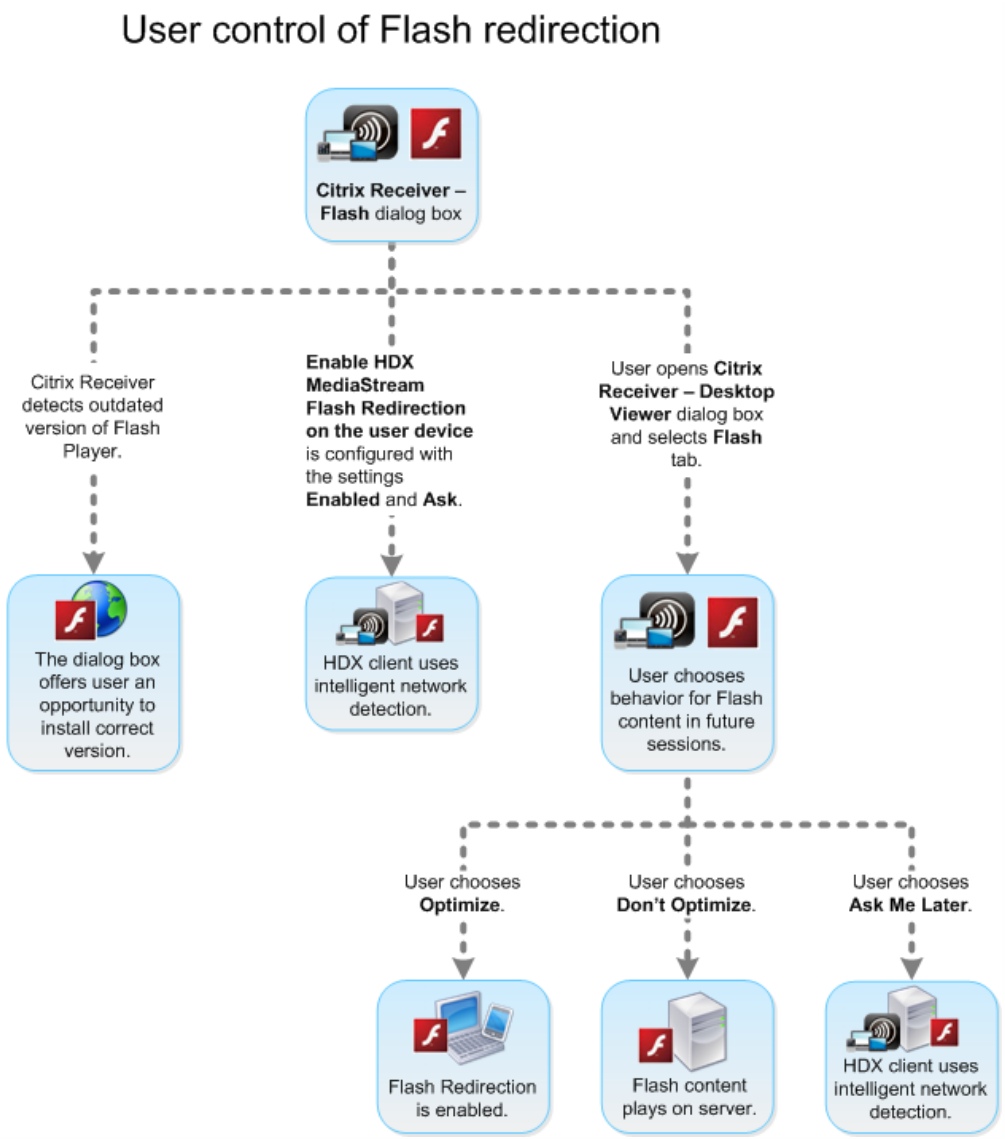
 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

intelligente Netzwerkerkennung zur Beurteilung der Sicherheitsstufe des clientseitigen Netzwerks erfolgt. Wenn die Sicherheit des Netzwerks nicht bestimmt werden kann, erhält der Benutzer die Entscheidung über die Flash-Umleitung. Es erscheint eine Aufforderung, die Flash-Umleitung zu aktivieren bzw. zu deaktivieren.
Die folgende Abbildung zeigt, wie die Flash-Umleitung für verschiedene Netzwerktypen verarbeitet wird.




Benutzer können die intelligente Netzwerkerkennung über das Dialogfeld Citrix Receiver - Desktop Viewer-Einstellungen mit der Option Optimieren überschreiben oder über die Option Nicht optimieren auf der Registerkarte Flash. Welche Optionen zur Auswahl stehen, hängt davon ab, wie die Flash-Umleitung auf dem Benutzergerät konfiguriert ist (siehe folgende Abbildung).


© 1999-2017 Citrix Systems, Inc. All rights reserved.




**Synchronisieren der clientseitigen HTTP-Cookies mit den serverseitigen HTTP-Cookies**

Die Option zur serverseitigen HTTP-Cookie-Synchronisierung ist standardmäßig deaktiviert. Aktivieren Sie die Synchronisierung, um HTTP-Cookies vom Server herunterzuladen. Diese HTTP-Cookies werden dann für den clientseitigen Inhaltsabruf verwendet und können bei Bedarf von Sites mit Flash-Inhalten gelesen werden. Hinweis: Clientseitige Cookies werden bei der Synchronisierung nicht ersetzt; sie sind weiterhin verfügbar, wenn die Synchronisierungsrichtlinie zu einem späteren Zeitpunkt deaktiviert wird.

1. Wählen Sie aus der Einstellungsliste die Option Synchronisierung der clientseitigen HTTP-Cookies mit den serverseitigen HTTP-Cookies aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung).

**Aktivieren Sie den serverseitigen Inhaltsabruf.**

Bei der standardmäßigen Flash-Umleitung werden Flash-Inhalte auf das Benutzergerät heruntergeladen und dort wiedergegeben. Bei Aktivierung des serverseitigen Inhaltsabrufs werden die Flash-Inhalte zum Server heruntergeladen und dann an das Benutzergerät gesendet. Die Inhalte werden auf dem Benutzergerät wiedergegeben, sofern keine Richtlinie mit höherer Priorität dies verhindert, z. B. wenn eine Site durch die Richtlinieneinstellung Flash-URL-Kompatibilitätsliste blockiert wird.

Serverseitiger Inhaltsabruf wird häufig verwendet, wenn das Benutzergerät eine Verbindung zu internen Sites über

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

NetScaler Gateway herstellt und wenn das Benutzergerät keinen direkten Internetzugang hat.

Hinweis: Der serverseitige Inhaltsabruf unterstützt keine Flash-Anwendungen, die Real Time Messaging Protocol (RTMP) verwenden. Stattdessen wird die serverseitige Wiedergabe für solche Sites verwendet.
Die zweite Generation der Flash-Umleitung unterstützt drei Aktivierungsoptionen für den serverseitigen Inhaltsabruf. Zwei dieser Optionen umfassen das Zwischenspeichern serverseitiger Inhalte auf dem Benutzergerät, wodurch die Leistung verbessert wird, da wiederverwendeter Inhalt bereits wiedergabebereit auf dem Benutzergerät verfügbar ist. Der Inhalt dieses Caches wird separat von anderen HTTP-Inhalten auf dem Benutzergerät gespeichert.

Bei der Flash-Umleitung der zweiten Generation wird der Fallback auf serverseitigen Inhaltsabruf automatisch gestartet, wenn eine der Aktivierungsoptionen ausgewählt ist und der clientseitige Abruf von SWF-Dateien fehlschlägt.

Zum Aktivieren des serverseitigen Inhaltsabrufs müssen auf dem Clientgerät und dem Server Einstellungen festgelegt sein.

1. Wählen Sie in der Einstellungsliste den Eintrag Serverseitigen Inhaltsabruf aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung). Wenn Sie diese Einstellung aktivieren, wählen Sie eine der Optionen aus der Liste Serverseitiger Inhaltsabrufstatus:

| Option | Beschreibung |
|---|---|
| Deaktiviert | Deaktiviert serverseitigen Inhaltsabruf und überschreibt die Einstellung URL-Liste für serverseitigen Flash-Inhaltsabruf auf dem Server. Fallback auf serverseitigen Inhaltsabruf ist auch deaktiviert. |
| Aktiviert | Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar, aber der Inhalt wird nicht zwischengespeichert. |
| Aktiviert (permanentes Caching) | Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und von Sitzung zu Sitzung gespeichert. |
| Aktiviert (temporäres Caching) | Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und am Ende der Sitzung gelöscht. |

3. Aktivieren Sie auf dem Server die Richtlinieneinstellung URL-Liste für serverseitigen Flash-Inhaltsabruf und füllen Sie sie mit Ziel-URLs.

**Umleiten der Benutzergeräte für clientseitigen Inhaltsabruf an andere Server**

Sie können einen Versuch, Flash-Inhalte abzurufen, mit der Einstellung URL-Neuschreibregeln für clientseitigen Inhaltsabruf umleiten. Hierbei handelt es sich um ein Feature der Flash-Umleitung der zweiten Generation. Bei der Konfiguration dieses Features geben Sie zwei URL-Schemas an. Wenn das Benutzergerät versucht, Inhalte von einer Webseite abzurufen, die dem ersten Schema (dem URL-Übereinstimmungsschema) entspricht, werden sie an eine Webseite weitergeleitet, die mit dem zweiten Schema festgelegt wurde (dem Ersetzungsschema).

Mit dieser Einstellung können Sie die Auswirkungen von Inhaltsübermittlungsnetzwerken (Content Delivery Networks,

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

CDN) kompensieren. Manche Webseiten, die Flash-Inhalte bereitstellen, verwenden CDN-Umleitung, damit Benutzer den Inhalt vom nächstgelegenen Server in einer Gruppe von Servern, auf denen derselbe Inhalt zur Verfügung steht, abrufen können. Bei der Verwendung des clientseitigen Inhaltsabrufs der Flash-Umleitung wird der Flash-Inhalt vom Benutzergerät abgerufen, während der Rest der Webseite, auf der sich der Flash-Inhalt befindet, vom Server abgerufen wird. Wenn CDN verwendet wird, wird die Serveranfrage an den am nächsten gelegenen Server geleitet und die Benutzergerätanfrage geht an denselben Standort. Dies möglicherweise nicht der Speicherort ist, der dem Benutzergerät am nächsten liegt; je nach Entfernung, kann eine sichtbare Verzögerung zwischen dem Laden der Webseite und die Wiedergabe von Flash-Inhalten entstehen.

1. Wählen Sie in der Einstellungsliste den Eintrag URL-Neuschreibregeln für clientseitigen Inhaltsabruf und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert. Nicht konfiguriert ist der Standardwert; Deaktiviert bewirkt, dass alle URL-Neuschreibregeln des nächsten Schrittes ignoriert werden.
3. Wenn Sie die Einstellung aktivieren, klicken Sie auf Anzeigen. Verwenden Sie die Perl-Syntax für reguläre Ausdrücke und geben Sie das URL-Schema im Feld Wert und das neu geschriebene URL-Format im Feld Wert ein.

### Angabe erforderlicher Mindestversionen für Flash-Umleitung

Sie können Registrierungseinstellungen hinzufügen, um die erforderliche Mindestversion für die Flash-Umleitung für Clientgeräte festzulegen, die auf VDAs mit Citrix Receiver für Windows oder Citrix Receiver für Linux zugreifen.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und ein erneutes Installieren des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

**ServerFlashPlayerVersionMinimum** ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Server (VDA) angibt.

**ClientFlashPlayerVersionMinimum** ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Client (Citrix Receiver) angibt.

Diese Versionszeichenfolgen können als "10", "10.2" oder "10.2.140" angegeben werden. Zurzeit werden nur die Hauptversions-, Nebenversions- und Buildnummern verglichen. Die Revisionsnummer wird ignoriert. Bei der Angabe von "10" als Versionszeichenfolge mit ausschließlicher Angabe der Hauptversionsnummer wird für die Nebenversions- und Buildnummer von 0 ausgegangen.

**FlashPlayerVersionComparisonMask** ist ein DWORD-Wert, der, wenn auf 0 festgelegt wird, den Vergleich der Flash Player-Version auf dem ICA-Client mit der auf dem ICA-Server deaktiviert. Die Vergleichsmaske hat auch andere Werte, die jedoch nicht verwendet werden sollten, da sich die Bedeutung jeder Maske mit einem Wert ungleich 0 ändern kann. Es wird empfohlen, die Vergleichsmaske für die gewünschten Clients nur auf 0 festzulegen. Es ist nicht empfehlenswert, die Vergleichsmaske unter den clientagnostischen Einstellungen festzulegen. Wenn keine Vergleichsmaske festgelegt ist, erfordert die Flash-Umleitung auf dem ICA-Client dieselbe Flash Player-Version wie auf dem ICA-Server oder eine höhere Version. Hierfür wird nur die Hauptversionsnummer verglichen.

Für die Umleitung müssen neben der Prüfung anhand der Vergleichsmaske die Prüfungen auf Mindestversion auf Client und Server bestanden werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Der Unterschlüssel "ClientID0x51" gibt den Linux-ICA-Client an. Der Unterschlüssel "ClientID0x1" gibt den Windows-ICA-Client an. Der Name des Unterschlüssels entsteht durch Anfügen der hexadezimalen Clientprodukt-ID (ohne führende Nullen) an die Zeichenfolge "ClientID". Eine vollständige Liste der Client-IDs enthält die Dokumentation zum Mobilen SDK für Windows Apps unter http://www.citrix.com/mobilitysdk/docs/clientdetection.html.

**Beispiel für eine 32-Bit-VDA-Registrierungskonfiguration**

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] clientagnostische Einstellungen

"ClientFlashPlayerVersionMinimum"="13.0" Mindestversion für ICA-Client "ServerFlashPlayerVersionMinimum"="13.0" Mindestversion für ICA-Server
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows-ICA-Client-Einstellungen

"ClientFlashPlayerVersionMinimum"="16.0.0" Gibt die Flash-Player-Mindestversion für den Windows-Client an
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux-ICA-Clienteinstellungen

"FlashPlayerVersionComparisonMask"=dword:00000000 Deaktiviert den Versionsvergleich für den Linux-Client (Prüfung, um festzustellen, ob die Flash Player-Version auf dem Client neuer ist als auf dem Server)
"ClientFlashPlayerVersionMinimum"="11.2.0" Flash Player-Mindestversion für Linux-Client.

**Beispiel für eine 64-Bit-VDA-Registrierungskonfiguration**

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# GPU-Beschleunigung für Windows Desktopbetriebssysteme

Jul 15, 2016

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Desktopbetriebssystemmaschinen bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen), XenServer-VMs mit GPU-Passthrough und XenServer-VMs mit virtuellem GPU (vGPU).

Mit XenServer GPU-Passthrough können Sie VMs mit exklusivem Zugriff auf dedizierte Hardware für die Grafikverarbeitung erstellen. Sie können mehrere GPUs auf dem Hypervisor installieren und VMs jeder dieser GPUs einzeln zuweisen.

Mit XenServer vGPU können mehrere virtuelle Maschinen die Grafikverarbeitungsleistung eines einzelnen physischen GPU direkt nutzen. Echtes Hardware-GPU Sharing bietet vollständige Windows 7- oder Windows 10-Desktops für Benutzer mit komplexen und anspruchsvollen Designanforderungen. Es wird für NVIDIA GRID-Karten unterstützt (siehe NVIDIA GRID) und verwendet die gleichen NVIDIA-Grafiktreiber, die unter nicht-virtualisierten Betriebssystemen bereitgestellt werden. Darüber hinaus wird sie für Intel-CPUs der Generationen 5 und 6 mit Intel Iris Pro unterstützt. Weitere Informationen zu den unterstützten Intel-Prozessoren finden Sie unter Intel Core-Prozessoren der fünften Generation und Intel Core i5-Prozessoren der sechsten Generation.

HDX 3D Pro bietet die folgenden Features:

- Adaptive, auf dem H.264-Standard basierende Tiefenkomprimierung für optimale Leistung bei WAN-Verbindungen und drahtlosen Verbindungen. HDX 3D Pro verwendet die auf CPU basierende Tiefenkomprimierung als Standardkomprimierungsverfahren zur Verschlüsselung. Dadurch wird eine optimale Komprimierung gewährleistet, die sich dynamisch an die Netzwerkbedingungen anpasst.
  Der auf dem H.264-Standard basierende Tiefenkomprimierungscodec konkurriert nicht mehr mit der Grafikwiedergabe um CUDA-Kerne auf der NVIDIA-GPU. Der Tiefenkomprimierungscodec wird auf der CPU ausgeführt und bietet Bandbreiteneffizienz.

- Verlustfreie Komprimierung für besondere Anwendungsfälle. HDX 3D Pro bietet einen verlustfreien CPU-basierten Codec zur Unterstützung von Anwendungen, in denen pixelgenaue Grafiken unerlässlich sind, z. B. für die medizinische Bilderstellung. Verlustfreie Komprimierung wird nur für besondere Anwendungsfälle empfohlen, da sie wesentlich mehr Netzwerk- und Verarbeitungsressourcen benötigt.
  Bei Verwendung von verlustfreier Komprimierung:
  - Die Anzeige für Verlustfreiheit, ein Symbol in der Taskleiste, zeigt an, ob es sich bei der Bildschirmanzeige um einen verlustreichen oder verlustfreien Frame handelt. Dies ist hilfreich, wenn die Richtlinieneinstellung Bildqualität auf Zu verlustfrei verbessern festgelegt ist. Die Anzeige für Verlustfreiheit wird grün, wenn die gesendeten Frames verlustfrei sind.
  - Über die Umschaltung für Verlustfreiheit können die Benutzer jederzeit innerhalb der Sitzung in den immer verlustfreien Modus wechseln. Zum Aktivieren oder Deaktivieren des verlustfreien Modus in einer Sitzung können Sie jederzeit mit der rechten Maustaste auf das Symbol klicken oder verwenden Sie die Tastenkombination ALT + UMSCHALT + 1.
    Für verlustfreie Komprimierung: HDX 3D Pro verwendet den verlustfreien Codec für die Komprimierung unabhängig von dem durch die Richtlinie ausgewählten Codec.

    Für die verlustreiche Komprimierung: HDX 3D Pro verwendet den ursprünglichen Codec, entweder den Standard oder den über die Richtlinie ausgewählten Codec.

    Einstellungen für die Umschaltung für Verlustfreiheit werden nicht für zukünftige Sitzungen gespeichert. Wenn Sie für alle Verbindungen den verlustfreien Codec verwenden möchten, legen Sie für die Richtlinie Bildqualität die Einstellung Immer verlustfrei fest.

- Sie können die Standardtastenkombination ALT + UMSCHALT + 1 zum Aktivieren oder Deaktivieren der Option "Verlustfrei" in einer Sitzung außer Kraft setzen. Konfigurieren Sie eine neue Registrierungseinstellung unter HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKLM_HotKey, Typ: String
  - Das Format beim Konfigurieren einer Tastenkombination ist C=0|1, A=0|1, S=0|1, W=0|1, K=val. Schlüssel müssen durch Kommata (,) getrennt werden. Die Reihenfolge der Tasten ist egal.
  - A, C, S, W und K sind Tasten, wobei Folgendes gilt: C=STRG, A=ALT, S=UMSCHALT, W=Win und K=eine gültige Taste. Zulässige Werte für K sind a-z, 0-9 und jeder virtuelle Tastencode. Weitere Informationen zu virtuellen Tastencodes finden Sie auf MSDN unter Virtual-Key Codes.
  - Beispiel:
    - Taste F10 entspricht K=0x79


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Taste STRG + F10 entspricht C=1, K=0x79
- ALT + A entspricht A=1, K=a oder A=1, K=A oder K=A, A=1
- STRG + ALT + 5 entspricht C=1, A=1, K=5 oder A=1, K=5, C=1
- STRG + UMSCHALT + F5 entspricht A=1, S=1, K=0x74

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

- Unterstützung für mehrere Monitore und hochauflösende Monitore: Für Windows 10-, Windows 8- und Windows 7-Desktops unterstützt HDX 3D Pro Benutzergeräte mit bis zu vier Monitoren. Benutzer können ihre Monitore beliebig konfigurieren sowie Monitore mit unterschiedlichen Auflösungen und Ausrichtungen kombinieren. Die Anzahl der Monitore wird nur durch die Leistungsfähigkeit des GPU auf dem Hostcomputer, des Benutzergeräts und der verfügbaren Bandbreite begrenzt. HDX 3D Pro unterstützt alle Monitorauflösungen. Einschränkungen bestehen nur hinsichtlich der Leistungsfähigkeit der GPU auf dem Hostcomputer.
  Auf Windows XP-Desktops bietet HDX 3D Pro eingeschränkte Unterstützung für Dual-Monitor-Zugriff. Weitere Informationen hierzu finden Sie unter VDAs auf Maschinen mit Windows XP oder Windows Vista.

- Dynamische Auflösung: Sie können Sie das Fenster des virtuellen Desktops oder der Anwendung auf eine beliebige Auflösung vergrößern oder verkleinern. **Hinweis**: Die einzige unterstützte Methode hierfür ist die Änderung der Größe des VDA-Sitzungsfensters. Das Ändern der Auflösung in der VDA-Sitzung (über "Systemsteuerung" > "Darstellung und Anpassung" > "Anzeige" > "Bildschirmauflösung") wird nicht unterstützt.

- Unterstützung für die NVIDIA-Kepler-Architektur: HDX 3D Pro unterstützt NVIDIA GRID-Karten (siehe NVIDIA GRID) für GPU-Passthrough und GPU Sharing. Der NVIDIA GRID-vGPU ermöglicht mehreren VMs den gleichzeitigen direkten Zugriff auf einen physischen GPU und die Verwendung derselben NVIDIA-Grafiktreiber, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden.
- Unterstützung für VMware vSphere und VMware ESX mit Virtual Direct Graphics Acceleration (vDGA): Sie können HDX 3D Pro mit vDGA sowohl für Remotedesktopdienste- als auch für VDI-Arbeitslasten verwenden.
- Unterstützung für Intel-CPUs der Generationen 5 und 6 mit Intel Iris Pro: HDX 3D Pro unterstützt den Betrieb von bis zu drei Bildschirmen, Console Blanking, benutzerdefinierte Auflösungen und hohe Frameraten. Weitere Informationen zu den unterstützten Intel-Prozessoren finden Sie unter Intel Core-Prozessoren der fünften Generation und Intel Core i5-Prozessoren der sechsten Generation.

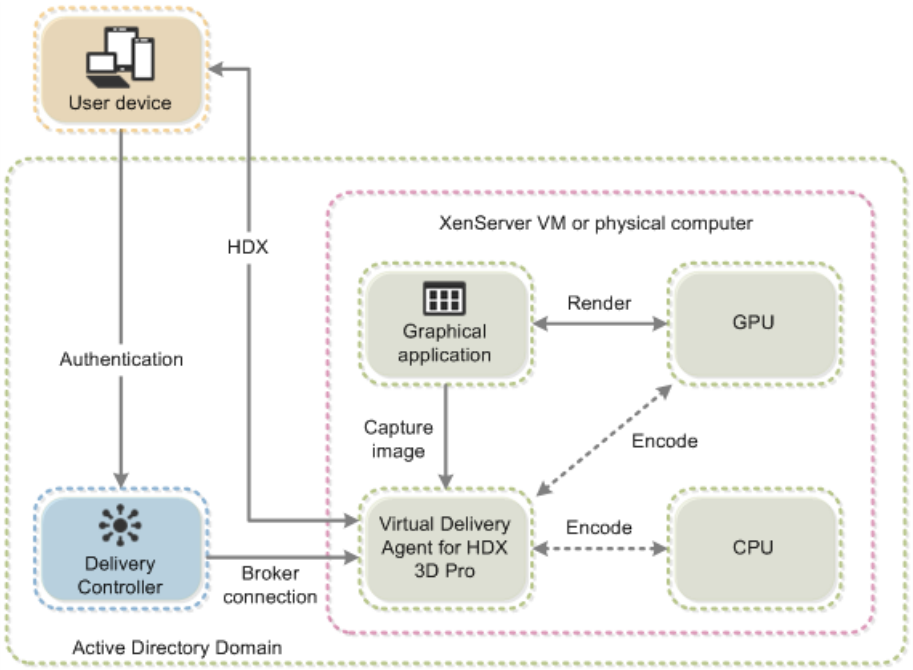
Wie in der folgenden Abbildung dargestellt:

- Der Hostcomputer muss sich in derselben Active Directory-Domäne wie der Delivery Controller befinden.
- Wenn sich ein Benutzer bei Citrix Receiver anmeldet und auf die virtuelle Anwendung oder den Desktop zugreift, authentifiziert der Controller den Benutzer und kontaktiert den VDA für HDX 3D Pro, um eine Verbindung zum Computer, der die grafische Anwendung hostet, zu vermitteln.

  Der VDA für HDX 3D Pro komprimiert mit der entsprechenden Hardware auf dem Host die Ansicht des gesamten Desktops oder nur der grafischen Anwendung.

- Die Desktop- oder Anwendungsansichten und die dazugehörigen Interaktionen der Benutzer werden zwischen dem Hostcomputer und dem Benutzergerät über eine direkte HDX-Verbindung zwischen Citrix Receiver und VDA für HDX 3D Pro übertragen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




## Installieren des VDA für HDX 3D Pro

Wenn Sie mit der grafischen Benutzeroberfläche des Installationsprogramms einen VDA für Windows-Desktopbetriebssysteme installieren, wählen Sie Ja auf der Seite "HDX 3D Pro". Wenn Sie die Befehlszeilenschnittstelle verwenden, schließen Sie die Option /enable_hdx_3d_pro in den Befehl XenDesktop VdaSetup.exe ein.

Für das Upgrade von HDX 3D Pro müssen Sie die separate Komponente HDX 3D für professionelle Grafiken und den VDA deinstallieren, bevor Sie den VDA für HDX 3D Pro installieren. Ebenso müssen Sie zum Wechsel vom standardmäßigen VDA zum VDA für HDX 3D Pro vor der Installation von VDA für HDX 3D Pro den standardmäßigen VDA deinstallieren.

## Installieren und Aktualisieren von NVIDIA-Treibern

Die NVIDIA GRID-API bietet direkten Zugriff auf den Framepuffer des Grafikprozessors und bietet die schnellste Framerate für eine gleichmäßige und interaktive Benutzererfahrung. Wenn Sie NVIDIA-Treiber vor einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID standardmäßig aktiviert.

Zum Aktivieren von NVIDIA GRID auf einer virtuellen Maschine müssen Sie den Microsoft Basic Display Adapter im Geräte-Manager deaktivieren. Führen Sie den folgenden Befehl aus und starten Sie dann den VDA neu: Montereyenable.exe –enable –noreset

Wenn Sie NVIDIA-Treiber nach einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID deaktiviert. Aktivieren Sie NVIDIA GRID mit dem von NVIDIA bereitgestellten Tool Montereryenable.

Führen Sie den folgenden Befehl aus, um NVIDIA GRID zu deaktivieren, und starten Sie dann den VDA neu: Montereyenable.exe –disable –noreset

## Installieren von Intel-Treibern

Dieser Schritt ist nur erforderlich, wenn Sie Intel-Treiber nach der Installation eines VDA mit HDX 3D Pro installieren oder wenn der Intel-Treiber aktualisiert wurde.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zum Aktivieren der Intel-Treiber für Multimonitorunterstützung führen Sie mit GfxDisplayTool.exe den folgenden Befehl aus und starten Sie dann den VDA neu: **GfxDisplayTool.exe -vd enable**.

GfxDisplayTool.exe ist im VDA-Installationsprogramm enthalten. GfxDisplayTool.exe ist in C:\Programme\Citrix\ICAServices.

> **Hinweis**
>
> Das Deinstallieren von NVIDIA- oder Intel-Treibern in ICA-Sitzungen wird nicht unterstützt.

## Optimierung der HDX 3D Pro-Benutzererfahrung

Stellen Sie bei der Verwendung von HDX 3D Pro mit mehreren Monitoren sicher, dass der Hostcomputer mit mindestens so vielen Monitoren konfiguriert ist, wie an den Geräten der Benutzer angeschlossen sind. Die an den Hostcomputer angeschlossenen Monitore können physikalische oder virtuelle Monitore sein.

Schließen Sie Monitore (physikalische oder virtuelle) nicht an Hostcomputer an, während Benutzer mit dem virtuellen Desktop oder der virtuellen Anwendung, die die grafische Anwendung bereitstellen, verbunden sind. Dies kann für die Dauer der Benutzersitzung zu Instabilität führen.

Teilen Sie den Benutzern mit, dass das Ausführen von Änderungen (von ihnen oder einer Anwendung) an der Desktopauflösung, während eine grafische Anwendungssitzung ausgeführt wird, nicht unterstützt wird. Nach dem Beenden der Anwendungssitzung können Benutzer die Auflösung des Desktop Viewer-Fensters in "Citrix Receiver - Desktop Viewer-Einstellungen" ändern.

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfiehlt Citrix die Verwendung der Richtlinieneinstellung Bandbreitenlimit für Sitzung insgesamt, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. Damit wird sichergestellt, dass die verfügbare Bandbreite beim Anmelden und Abmelden der Benutzer keinen großen Schwankungen unterworfen ist. Da HDX 3D Pro automatische Anpassungen durchführt, um die gesamte Bandbreite auszuschöpfen, kann sich die stark variierende verfügbare Bandbreite während der Benutzersitzungen negativ auf die Leistung auswirken.

Wenn beispielsweise 20 Benutzer eine Verbindung mit 60 MBit/s gemeinsam verwenden, kann die Bandbreite, die den einzelnen Benutzern zur Verfügung steht, abhängig von der Anzahl der gleichzeitigen Benutzer zwischen 3 MBit/s und 60 MBit/s variieren. Um die Benutzererfahrung in diesem Szenario zu optimieren, legen Sie die Bandbreite fest, die zu Spitzenzeiten pro Benutzer erforderlich ist, und stellen Sie sicher, dass die Benutzer diesen Wert nicht überschreiten können.

Citrix empfiehlt Benutzern einer 3D-Maus, die Priorität des virtuellen Kanals für die generische USB-Umleitung auf 0 zu erhöhen. Weitere Informationen dazu, wie Sie die Priorität virtueller Kanäle ändern können, finden Sie unter CTX128190.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# GPU-Beschleunigung für Windows-Serverbetriebssystem

Jul 08, 2016

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Windows-Serverbetriebssystemsitzungen ausgeführt werden, auf der GPU des Servers wiedergegeben werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Zusätzlich kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

Bei Verwendung von HDX 3D Pro können mehrere Benutzer eine Grafikkarte gemeinsam verwenden. Wenn HDX 3D Pro mit XenServer GPU-Passthrough verwendet wird, hostet ein Server mehrere Grafikkarten, d. h. eine pro virtuelle Maschine.

Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

## GPU Sharing

GPU Sharing ermöglicht die GPU-Hardwarewiedergabe von OpenGL- und DirectX-Anwendungen in Remotedesktopsitzungen und hat die folgenden Merkmale:

- Verwenden auf Bare-Metal- oder virtuellen Maschinen, um die Anwendungsskalierbarkeit und -leistung zu steigern.
- Mehrere gleichzeitige Sitzungen können GPU-Ressourcen gemeinsam verwenden. (Die meisten Benutzer benötigen nicht die Wiedergabeleistung eines dedizierten GPU).
- Erfordert keine besonderen Einstellungen.

Sie können mehrere GPUs auf einem Hypervisor installieren und jedem GPU eine VM zuordnen: entweder durch Installation einer Grafikkarte mit mehreren GPUs oder durch Installation mehrerer Grafikkarten mit einem oder mehreren GPUs. Eine Mischung heterogener Grafikkarten auf einem Server wird nicht empfohlen.

Virtuelle Maschinen benötigen einen direkten Passthrough-Zugriff auf einen GPU; dies ist mit Citrix XenServer oder VMware vSphere verfügbar. Wenn HDX 3D mit GPU-Passthrough verwendet wird, unterstützt jeder GPU des Servers eine virtuelle Maschine mit mehreren Benutzern.

GPU Sharing hängt nicht von einer bestimmten Grafikkarte ab.

- Wählen Sie bei Ausführung auf einem Hypervisor eine Hardwareplattform und Grafikkarten aus, die mit der Implementierung von GPU-Passthrough des Hypervisors kompatibel sind. Die Liste der Hardware, die Zertifizierungstests mit XenServer GPU-Passthrough bestanden hat, finden Sie unter GPU-Passthroughgeräte.
- Bei Ausführung auf Bare-Metal sollte eine Grafikkarte vom Betriebssystem aktiviert sein. Wenn mehrere GPUs auf der Hardware installiert sind, deaktivieren Sie mit dem Device Manager alle außer einem.

Die Skalierbarkeit mit GPU Sharing hängt von folgenden Faktoren ab:

- Ausgeführte Anwendungen
- Verbrauchter Videospeicher
- Verarbeitungsleistung der Grafikkarte


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Beispiel: Skalierbarkeitswerte im Bereich von 8 bis 10 Benutzern wurden für NVIDIA Q6000- und M2070Q-Karten berichtet, die Anwendungen wie ESRI ArcGIS ausführen. Diese Karten haben 6 GB Videospeicher. Neuere NVIDIA GRID-Karten haben 8 GB Videospeicher und eine wesentlich höhere Verarbeitungsleistung (mehr CUDA-Kerne). Bei NVIDIA GRID K2-Karten wurde bei bis zu 20 Benutzern pro GRID K2-Karte eine gute Leistung beobachtet. Bei anderen Anwendungen kann die Skalierbarkeit wesentlich höher liegen; sie können 32 gleichzeitige Benutzer bei einem Profi-GPU erreichen.

Einige Anwendungen handhaben fehlenden Videospeicher besser als andere. Wenn die Hardware stark überlastet wird, kann der Grafikkartentreiber instabil werden oder abstürzen. Schränken Sie die Anzahl der gleichzeitigen Benutzer ein, um diese Probleme zu vermeiden.

Sie können die GPU-Beschleunigung mit einem Tool von Drittanbietern bestätigen, z. B. GPU-Z. GPU-Z finden Sie unter http://www.techpowerup.com/gpuz/.

### Wiedergabe von DirectX, Direct3D und WPF

Die Wiedergabe von DirectX, Direct3D und WPF steht nur auf Servern zur Verfügung, die einen Grafikprozessor haben, der eine Anzeigetreiberschnittstelle der Version 9ex, 10 oder 11 unterstützt.

- Unter Windows Server 2008 R2 sind für DirectX und Direct3D keine Sondereinstellungen erforderlich, um einen einzelnen GPU zu verwenden.
- Unter Windows Server 2012 verwenden Remotedesktopdienste-Sitzungen auf dem RD-Sitzungshostserver als Standardadapter den Microsoft Basic Render-Treiber. Um den GPU in RDS-Sitzungen unter Windows Server 2012 zu verwenden, aktivieren Sie die Einstellung Use the hardware default graphics adapter for all Remote Desktop Services sessions in der Gruppenrichtlinie "Lokale Computerrichtlinie > Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung".
- Um die Wiedergabe von WPF-Anwendungen mit der GPU des Servers zu aktivieren, müssen Sie in der Registrierung des Servers, der die Windows-Serverbetriebssystemsitzungen ausführt, die folgenden Einstellungen erstellen:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

### GPU-Beschleunigung für CUDA- oder OpenCL-Anwendungen

Die GPU-Beschleunigung von CUDA- und OpenCL-Anwendung, die in einer Benutzersitzung ausgeführt werden, wird nur als Machbarkeitsstudie unterstützt. Diese Unterstützung ist in der Standardeinstellung deaktiviert, Sie können sie jedoch für Test- und Evaluierungszwecke aktivieren.

Aktivieren Sie die folgenden Registrierungseinstellungen, um die im Rahmen der Machbarkeitsstudie verfügbaren CUDA-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

Aktivieren Sie die folgenden Registrierungseinstellungen, um die im Rahmen der Machbarkeitsstudie verfügbaren OpenCL-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# OpenGL Software Accelerator

Jul 08, 2016

OpenGL Software Accelerator ist ein Softwarerasterizer für OpenGL-Anwendungen wie ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD und CAM. In einigen Fällen bietet OpenGL Software Accelerator auch ohne die Verwendung einer Grafikkarte eine gute Benutzererfahrung mit OpenGL-Anwendungen.

Wichtig: OpenGL Software Accelerator wird ohne Modifikation bereitgestellt und muss für alle Anwendungen getestet werden. Er funktioniert möglicherweise mit einigen Anwendungen nicht, kann aber als Lösung dienen, wenn der Windows OpenGL-Rasterizer keine angemessene Leistung bietet. Wenn OpenGL Software Accelerator mit Ihren Anwendungen funktioniert, kann es Ihnen Kosten für GPU-Hardware sparen.

OpenGL Software Accelerator ist im Ordner "Support" auf dem Installationsmedium und wird auf allen gültigen VDA-Plattformen unterstützt.

Einsatzmöglichkeiten für OpenGL Software Accelerator

- Wenn die Leistung von OpenGL-Anwendungen in virtuellen Maschinen auf XenServer oder anderen Hypervisors unzureichend ist, verwenden Sie OpenGL Accelerator. Bei einigen Anwendungen werden mit OpenGL Accelerator durch den Einsatz von SSE4.1 und AVX bessere Ergebnisse erzielt als mit dem in Windows enthaltenen Microsoft OpenGL Rasterizer. OpenGL Accelerator unterstützt zudem Anwendungen, die OpenGL-Versionen bis 2.1 verwenden.
- Bei Anwendungen, die auf einer Arbeitsstation ausgeführt werden, sollte zunächst die Standardversion von OpenGL verwendet werden, die von der Arbeitsstation des Grafikadapters bereitgestellt wird. Wenn es sich um eine aktuelle Grafikkarte handelt, wird damit in den meisten Fällen die beste Leistung erzielt. Bei Grafikkarten älterer Versionen oder weniger leistungsstarken Grafikkarten sollte OpenGL Software Accelerator eingesetzt werden.
- 3D OpenGL-Anwendungen, die nicht angemessen bereitgestellt wurden und CPU-basierte Softwarerasterisierung verwenden, profitieren möglicherweise von der OpenGL GPU-Hardwarebeschleunigung. Dieses Feature kann auf Bare-Metal- oder virtuellen Maschinen verwendet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Audiofeatures

Jul 08, 2016

Sie können die folgenden Citrix Richtlinieneinstellungen konfigurieren und einer Richtlinie hinzufügen, mit der HDX-Audiofeatures optimiert werden. Nutzungsinformationen sowie Beziehungen mit und Abhängigkeiten von anderen Richtlinieneinstellungen finden Sie in den Artikeln Einstellungen der Richtlinie "Audio", Einstellungen der Richtlinie "Bandbreite" und Einstellungen der Richtlinie "Multistreamverbindungen".

Wichtig: Die meisten Audiofeatures werden über den ICA-Stream transportiert und werden auf dieselbe Weise gesichert wie anderer ICA-Datenverkehr. Bei UDP (User Datagram Protocol) wird ein separater, ungesicherter Übertragungsmechanismus verwendet, wenn NetScaler Access Gateway nicht im Pfad ist. Ist NetScaler Access Gateway für den Zugriff auf XenApp- und XenDesktop-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und NetScaler Access Gateway mittels DTLS gesichert.

## Audioqualität

Im Allgemeinen erfordert eine höhere Audioqualität mehr Bandbreite und führt zu einer höheren CPU-Auslastung, da mehr Audiodaten an die Benutzergeräte gesendet werden. Mit der Audiokomprimierung können Sie die Audioqualität und die Sitzungsleistung aufeinander abstimmen; verwenden Sie Citrix Richtlinieneinstellungen, um den Komprimierungsgrad für Audiodateien zu konfigurieren.

Standardmäßig ist die Richtlinieneinstellung Audioqualität auf Hoch - High Definition-Audio eingestellt. Diese Einstellung bietet HiFi-Stereo-Audio, verbraucht aber mehr Bandbreite als die anderen Einstellungen. Verwenden Sie diese Audioqualität nicht für nicht optimierte Chat- und Videochat-Anwendungen (z. B. Softphones), da es hierbei zu Verzögerungen im Audiopfad kommen kann, was bei Echtzeitkommunikation ungeeignet ist.

Sie können auch die Erstellung separater Richtlinien für Benutzergruppen mit Einwählverbindungen und für Benutzer, die über ein LAN oder WAN eine Verbindung herstellen, in Erwägung ziehen. Benutzern ist bei DFÜ-Verbindungen, bei denen die Bandbreite im Allgemeinen begrenzt ist, die Download-Geschwindigkeit gewöhnlich wichtiger als die Audioqualität. Erstellen Sie daher für DFÜ-Verbindungen eine Richtlinie, die für Audio einen hohen Komprimierungsgrad anwendet, sowie eine weitere Richtlinie für LAN- oder WAN-Verbindungen, die einen geringen Komprimierungsgrad anwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

## Clientaudioumleitung

Damit der Audioempfang von einer Anwendung auf dem Server über Lautsprecher oder andere Soundgeräte (z. B. Kopfhörer) auf dem Benutzergerät zugelassen wird, fügen Sie die Einstellung Clientaudioumleitung hinzu, die standardmäßig zugelassen ist.

Die Clientaudiozuordnung kann dazu führen, dass eine hohe Last auf dem Server und dem Netzwerk entsteht. Durch Nichtzulassen der Clientaudioumleitung werden jedoch alle HDX-Audiofunktionen deaktiviert.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

## Clientmikrofonumleitung

Damit die Audioaufzeichnung mit Eingabegeräten wie Mikrofonen auf dem Benutzergerät zugelassen wird, fügen Sie die Einstellung Clientmikrofonumleitung hinzu, die standardmäßig zugelassen ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Benutzergeräten haben, auf Mikrofone zugreifen und können dann den Zugriff vor Verwenden des Mikrofons akzeptieren oder ablehnen. Benutzer können die diesbezügliche Warnung in Citrix Receiver deaktivieren.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

### Audio Plug & Play

Die Richtlinie Audio Plug & Play steuert, ob mehrere Audiogeräte zum Aufzeichnen und Wiedergeben zulässig sind. Diese Einstellung ist standardmäßig aktiviert.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio".

### Bandbreitenlimit für die Audioumleitung und Bandbreitenlimit für die Audioumleitung (Prozent)

Die Richtlinieneinstellung Bandbreitenlimit für die Audioumleitung gibt die maximale Bandbreite (in Kilobits pro Sekunde) für die Wiedergabe und Aufzeichnung von Audio in einer Sitzung an. Die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) gibt die maximale Bandbreite für die Umleitung als Prozentsatz der insgesamt verfügbaren Bandbreite an. Standardmäßig ist Null (Maximum) für beide Einstellungen angegeben. Wenn beide Einstellungen konfiguriert sind, wird die Einstellung mit dem niedrigsten Bandbreitenlimit verwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Bandbreite". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

### Audio über UDP - Real-time Transport und Audio-UDP-Portbereich

Standardmäßig ist Audio über UDP - Real-time Transport auf "Zugelassen" eingestellt (sofern die entsprechende Option bei der Installation ausgewählt wurde), sodass ein UDP-Port auf dem Server für alle Verbindungen geöffnet wird, die für die Echtzeitübertragung von Audio über UDP konfiguriert wurden. Citrix empfiehlt, dass Sie UDP/RTP für Audio konfigurieren, um auch bei Netzwerküberlastung oder Paketverlust die beste Benutzererfahrung sicherzustellen.
Wichtig: Mit UDP übertragene Audiodaten werden nicht verschlüsselt, wenn NetScaler Access Gateway nicht im Pfad ist. Ist NetScaler Access Gateway für den Zugriff auf XenApp- und XenDesktop-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und NetScaler Access Gateway mittels DTLS gesichert.
Mit der Einstellung Audio-UDP-Portbereich geben Sie den Bereich der Portnummern an, die der Virtual Delivery Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet.

Standardmäßig ist der Bereich 16500 bis 16509.

Informationen zu den Einstellungen von "Audio über UDP - Real-time Transport" finden Sie unter Einstellungen der Richtlinie "Audio". Informationen zu "Audio-UDP-Portbereich" finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

### Audioeinstellungsrichtlinien für Benutzergeräte

1. Laden Sie die Gruppenrichtlinienvorlagen gemäß den Anleitungen unter Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage herunter.
2. Erweitern Sie im Gruppenrichtlinien-Editor "Administrative Vorlagen > Citrix Components > Citrix Receiver > User Experience".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie für Clientaudioeinstellungen die Option **Nicht konfiguriert**, **Aktiviert** oder **Deaktiviert**.
   - **Nicht konfiguriert**: Standardmäßig ist die Audioumleitung mit hoher Qualität oder zuvor konfigurierten benutzerdefinierten Audioeinstellungen aktiviert.
   - **Aktiviert**: Die Audioumleitung wird mit den ausgewählten Optionen aktiviert.
   - **Deaktiviert**: Die Audioumleitung wird deaktiviert.
4. Wenn Sie **Aktiviert** festlegen, wählen Sie eine Audioqualität. Verwenden Sie für UDP-Audio die Standardeinstellung **Mittel**.
5. Aktivieren Sie nur für UDP-Audio die Einstellung **Echtzeittransport aktivieren** und legen Sie den Bereich der eingehenden Ports so fest, dass der Durchgang durch die lokale Windows-Firewall gewährleistet ist.
6. Zur Verwendung von UDP-Audio mit NetScaler Access Gateway wählen Sie die Option **Echtzeittransport über Gateway zulassen**. NetScaler Access Gateway muss mit DTLS konfiguriert werden. Weitere Informationen finden Sie unter UDP Audio Through a Netscaler Gateway.

Wenn Sie als Administrator auf Endpunktgeräten solche Änderungen nicht vornehmen können (beispielsweise im Fall von BYOD-Geräten oder Heimcomputern), aktivieren Sie UDP-Audio über die default.ica-Attribute von StoreFront.

1. Öffnen Sie auf dem Computer mit StoreFront die Datei C:\inetpub\wwwroot\Citrix\\App_Data\default.ica in einem Texteditor.
2. Fügen Sie unter dem Abschnitt [Application] Folgendes hinzu:

command KOPIEREN

```
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

Wird UDP-Audio über die Datei default.ica aktiviert, gilt die Aktivierung für alle Benutzer des Stores.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Vermeiden von Echo in Multimediakonferenzen

Teilnehmer von Audio- oder Videokonferenzen hören eventuell ein Echo. Echos treten normalerweise auf, wenn der Abstand zwischen Lautsprechern und Mikrofonen nicht groß genug ist. Aus diesem Grund empfiehlt Citrix, dass Sie für Audio- und Videokonferenzen Kopfhörer verwenden.

HDX verfügt über eine Option zur Echounterdrückung (standardmäßig aktiviert), die das Auftreten von Echo minimiert. Die Qualität der Echounterdrückung hängt stark vom Abstand zwischen den Lautsprechern und dem Mikrofon ab. Der Abstand zwischen den Geräten darf nicht zu groß aber auch nicht zu klein sein.

Sie können eine Registrierungseinstellung ändern, um die Echounterdrückung zu deaktivieren. Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Navigieren Sie mit dem Registrierungs-Editor auf dem Benutzergerät zu einer der folgenden Optionen:
   - 32-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - 64-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Ändern Sie den Wert im Feld Wert zu FALSE.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Prioritäten für den Netzwerkdatenverkehr

Jul 08, 2016

Prioritäten für den Netzwerkdatenverkehr über mehrere Verbindungen für eine Sitzung werden zugewiesen, indem Diensteigenschaft(QoS)-fähige Router verwendet werden. Vier TCP/IP-Streams (real-time, interactive, background und bulk) und ein UDP/RTP-Stream (für Voice) sind zum Ausführen von ICA-Datenverkehr zwischen dem Benutzergerät und dem Server verfügbar. Jeder virtuelle Kanal ist mit einer bestimmten Priorität verknüpft und wird von der entsprechenden TCP-Verbindung transportiert. Sie können die Kanäle basierend auf der Portnummer, die für die Verbindung verwendet wird, unabhängig voneinander festlegen.

Gestreamte Mehrkanalverbindungen werden für Virtual Delivery Agents (VDAs) unterstützt, die auf Windows 8- und Windows 7-Maschinen installiert sind. Arbeiten Sie mit dem Netzwerkadministrator Ihres Unternehmens zusammen, um sicherzustellen, dass die in der Einstellung "Multiport-Richtlinie" konfigurierten Common Gateway Protocol (CGP)-Ports auf den Netzwerkroutern richtig zugewiesen sind.

Quality of Service wird nur unterstützt, wenn mehrere Sitzungszuverlässigkeitsports, oder CGP-Ports, konfiguriert sind.

Achtung: Verwenden Sie Transportsicherheit, wenn Sie dieses Feature einsetzen. Citrix empfiehlt die Verwendung von Internetprotokollsicherheit (IPsec) oder Transport Layer Security (TLS). TLS-Verbindungen werden nur unterstützt, wenn die Verbindungen durch ein NetScaler Gateway passieren, das Multistream unterstützt. Bei internen Unternehmensnetzwerken werden Multistreamverbindungen mit TLS nicht unterstützt.
Fügen Sie folgende Citrix Richtlinieneinstellungen einer Richtlinie hinzu, um die Servicequalität für mehrere Streamingverbindungen festzulegen (weitere Details finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen"):

- Multiportrichtlinie: Diese Einstellung legt Ports für den ICA-Verkehr über mehrere Verbindungen fest und definiert die Netzwerkpriorität.
  - Wählen Sie eine Priorität aus der Liste CGP-Standardportpriorität aus. Standardmäßig hat der primäre Port (2598) eine hohe Priorität.
  - Geben Sie in den Feldern CGP-Port1, CGP-Port2 und CGP-Port3 je nach Bedarf zusätzliche CGP-Ports sowie entsprechende Prioritäten ein. Jeder Port muss eine eindeutige Priorität haben.

  Konfigurieren Sie die Firewalls auf VDAs explizit so, dass zusätzlicher TCP-Datenverkehr zulässig ist.

- Multistreamcomputereinstellung: Diese Einstellung ist standardmäßig deaktiviert. Wenn Sie Citrix Cloudbridge mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.
- Multistreambenutzereinstellung: Diese Einstellung ist standardmäßig deaktiviert.

Damit die Richtlinien mit diesen Einstellungen wirksam werden, müssen sich Benutzer abmelden und dann am Netzwerk anmelden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überlegungen zu USB und Clientlaufwerk

Jul 08, 2016

Mit HDX USB-Geräteumleitung können Benutzer eine Verbindung zum USB-Flashlaufwerk auf einem lokalen Computer herstellen und dann remote von einem virtuellen Desktop oder einer desktopgehosteten Anwendung darauf zugreifen. Während einer Sitzung können Benutzer Plug-n-Play-Geräte verwenden, einschließlich PTP-Geräte (Picture Transfer Protocol) wie digitale Kameras, MTP-Geräte (Media Transfer Protocol) wie digitale Audio Player oder tragbare Media Player und POS-Geräte (Point of Sale).

Double-Hop-USB wird bei Sitzungen mit über Desktop gehosteten Anwendungen nicht unterstützt.

USB-Umleitung ist verfügbar für Citrix Receiver für Windows und Citrix Receiver für Linux.

Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Weitere Informationen hierzu finden Sie in der Citrix Receiver-Dokumentation. Sie können festlegen, welche USB-Geräte einem virtuellen Desktop verfügbar gemacht werden, indem Sie die Liste der unterstützten USB-Geräte für die Umleitung beschränken.

> **Important**
>
> In Umgebungen, in denen aus Sicherheitsgründen eine Trennung zwischen dem Benutzergerät und dem Server erforderlich ist, müssen Sie die Benutzer darüber informieren, welche Typen von USB-Geräten zu vermeiden sind.

Die beliebtesten USB-Geräte können über optimierte virtuelle Kanäle umgeleitet werden und liefern Leistung und Bandbreiteneffizienz über ein WAN. Der Grad der Unterstützung hängt vom auf dem Benutzergerät installierten Citrix Receiver ab. Optimierte virtuelle Kanäle sind normalerweise die beste Option, insbesondere in Umgebungen mit hoher Latenz.

Für die Umleitung von USB-Geräten gilt, dass ein SMART-Board ebenso wie eine Maus behandelt wird.

Das Produkt unterstützt die Verwendung von optimierten virtuellen Kanälen mit USB 3.0-Geräten und USB 3.0-Ports, wie ein virtueller CDM-Kanal, der zum Anzeigen von Dateien auf einer Kamera oder zur Audiowiedergabe über ein Headset verwendet wird. Das Produkt unterstützt zudem die generische USB-Umleitung von USB 3.0-Geräten, die mit einem USB 2.0-Port verbunden sind.

Spezialgeräte, für die es keine optimierten virtuellen Kanäle gibt, werden durch die Verwendung eines allgemeinen virtuellen Kanals für USB unterstützt, der eine unformatierte USB-Umleitung bietet. Informationen zu allen mit XenDesktop getesteten USB-Geräten finden Sie unter CTX123569.

Einige erweiterte gerätespezifischen Features, wie z. B. auf HID-Schaltflächen (Human Interface Device) auf einer Webcam, funktionieren möglicherweise mit dem optimierten virtuellen Kanal nicht wie erwartet. Wenn dies ein Problem darstellt, können Sie den allgemeinen virtuellen Kanal für USB verwenden.

Einige Geräte werden standardmäßig nicht umgeleitet und sind nur in der lokalen Sitzung verfügbar. Es wäre beispielsweise nicht angemessen, eine über internes USB an der Hauptplatine des Benutzergeräts angeschlossene Netzwerkkarte umzuleiten.

Die folgenden Citrix Richtlinieneinstellungen steuern die USB-Unterstützung:

- **Regeln für die Client-USB-Geräteoptimierung:** Der Optimierungsmodus wird für class=03-Eingabegeräte (z. B. Signaturgeräte oder Grafiktablets) unterstützt. Wenn keine Regel angegeben ist, wird das Gerät im interaktiven Modus behandelt (02). Aufnahmemodus (04) ist der empfohlene Modus für Signaturgeräte.
- **Client-USB-Geräteumleitung**: Standardeinstellung: "Nicht zugelassen".
- **Regeln für die Client-USB-Geräteumleitung**: Die Regeln gelten nur für Geräte, die generische USB-Umleitung verwenden, und nicht für Geräte, die spezielle oder optimierte Umleitung verwenden, wie CDM.
- **Client-USB-Geräteumleitung für Plug & Play-Geräte**: Die Standardeinstellung "Zugelassen" ermöglicht Plug & Play von PTP-, MTP- und POS-Geräten in einer Sitzung.
- **Bandbreitenlimit für Client-USB-Geräteumleitung**: Der Standardwert ist "0" (kein Maximum).
- **Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)**: Der Standardwert ist 0 (kein Maximum).

### Info zur generischen USB-Umleitung

Generische USB-Umleitung ist für spezielle USB-Geräte, für die es keinen optimierten virtuellen Kanal gibt. Diese Funktion leitet beliebige USB-Geräte von Clientmaschinen an virtuelle Desktops um. Durch dieses Feature können Endbenutzer mit vielen generischen USB-Geräten in der Desktopsitzung so interagieren, als wären die Geräte direkt angeschlossen.

Vorteile von generischer USB-Umleitung:

- Benutzer müssen keine Gerätetreiber auf den Benutzergeräten installieren.
- USB-Clienttreiber werden auf der VDA-Maschine installiert.

Dieses Feature wird für Desktopsitzungen auf VDAs für Desktop-OS ab Version 7.6 unterstützt.

Dieses Feature wird mit den folgenden Einschränkungen auch für Desktopsitzungen auf VDAs für Server-OS ab Version 7.6 unterstützt:

- Auf der VDA-Maschine muss Windows Server 2012 R2 ausgeführt werden
- Nur Single-Hop-Szenarios werden unterstützt
- Die USB-Clienttreiber müssen mit RDSH für Windows 2012 R2 kompatibel sein
- USB-Speichergeräte, Audiogeräte, Smartcardleser und Geräte, die nicht voll virtualisiert sind, werden nicht unterstützt

Weitere Informationen zur generischen USB-Umleitung finden Sie unter CTX137939.

### Aktivieren von USB-Unterstützung

1. Fügen Sie die Einstellung Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie den Wert auf Zugelassen ein.
2. (Optional) Zum Aktualisieren der für Remoting verfügbaren USB-Geräteliste fügen Sie die Einstellung Regeln für die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie die USB-Standardrichtlinienregeln ein.
3. Aktivieren Sie die USB-Unterstützung, wenn Sie Citrix Receiver auf Benutzergeräten installieren. Wenn Sie im vorigen Schritt die USB-Richtlinienregeln für den VDA festgelegt haben, geben Sie nun die gleichen Richtlinienregeln für Citrix Receiver ein. Informationen zur USB-Unterstützung Für Thin Clients und die erforderliche Konfiguration erhalten Sie vom Hersteller.

### Aktualisieren der für Remoting verfügbaren USB-Geräteliste (Citrix Receiver für Windows 4.2)

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden. USB-Geräte werden auch automatisch umgeleitet, wenn das Gerät im Modus "Desktop Appliance" ist und der Verbindungsbalken nicht angezeigt wird. In manchen Fällen empfiehlt es sich jedoch, die automatische Umleitung nicht für alle USB-Geräte zu aktivieren. Weitere Informationen finden Sie unter CTX123015.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Um zu verhindern, dass Geräte überhaupt aufgeführt oder umgeleitet werden, können Sie auf dem Client und für VDA die nachfolgenden Geräteregeln festlegen.

Sie können die USB-Geräte, die für Remoting verfügbar sind, aktualisieren, indem Sie Regeln für die Client-USB-Geräteumleitung für Citrix Receiver und VDA definieren, die dann die USB-Standardrichtlinienregeln außer Kraft setzen.

- Bearbeiten Sie die Benutzergeräteregistrierung. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Bearbeiten Sie die Administrator-Überschreibungsregeln der Serverbetriebssystemmaschinen mit den Gruppenrichtlinienregeln. Die Gruppenrichtlinien-Verwaltungskonsole ist auf dem Installationsmedium enthalten:
  - Für x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Für x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln, wie nachfolgend beschrieben. Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format {Allow:|Deny:} gefolgt von Tag=Wert-Ausdrücken, die durch Leerzeichen getrennt sind. Die folgenden Tags werden unterstützt:

| Tag | Beschreibung |
|---|---|
| VID | Vendor-ID vom Gerätedeskriptor |
| PID | Produkt-ID vom Gerätedeskriptor |
| REL | Release-ID vom Gerätedeskriptor |
| Klasse | Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter http://www.usb.org/. |
| SubClass | Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor |
| Prot | Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor |

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel; Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

> **Important**
>
> Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit Semikolons getrennt eingeben.

Bei optimierten Geräten, wie Massenspeichergeräten, wird das Gerät normalerweise über den speziellen CDM-Kanal umgeleitet und nicht mit Richtlinienregeln. Sie können dieses Verhalten auf die folgende Weise überschreiben:

- Leiten Sie das optimierte Gerät manuell mit der generischen USB-Umleitung um: Wählen Sie im Dialogfeld Einstellungen auf der Registerkarte Geräte die Option Zu allgemein wechseln.
- Leiten Sie das optimierte Gerät automatisch mit der generischen USB-Umleitung um, indem Sie die automatische Umleitung für das Speichergerät festlegen (z. B. AutoRedirectStorage = 1) und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfigurieren. Weitere Informationen finden Sie unter CTX123015.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Vendor- und Produkt-IDs:
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse  Deny: VID=046D # Deny all Logitech products
- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für eine definierte Klasse, Unterklasse und ein Protokoll:
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices  Allow: Class=EF SubClass=01 # Allow Sync devices  Allow: Class=EF # Allow all USB-Miscellaneous devices

### Aktualisieren der für Remoting verfügbaren USB-Geräteliste

Standardmäßig werden USB-Geräte automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden. USB-Geräte werden auch für Desktopgerätesites oder desktopgehostete Anwendungen automatisch umgeleitet. In manchen Fällen empfiehlt es sich jedoch, die automatische Umleitung nicht für alle USB-Geräte zu aktivieren. Weitere Informationen finden Sie unter CTX123015.

Benutzer von Desktop Viewer können Geräte umleiten, die nicht automatisch umgeleitet werden, indem Sie sie aus der USB-Geräteliste auswählen. Um zu verhindern, dass Geräte aufgeführt oder umgeleitet werden, legen Sie auf dem Benutzergerät und dem VDA die Geräteregeln fest.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sie können die USB-Geräte, die für Remoting verfügbar sind, aktualisieren, indem Sie Regeln für die Client-USB-Geräteumleitung für Citrix Receiver und VDA definieren, die dann die USB-Standardrichtlinienregeln außer Kraft setzen. Geräteregeln werden sowohl für Citrix Receiver als auch Virtual Desktop Agent zwingend umgesetzt. Achten Sie darauf, die Regeln für beide zu ändern, damit die Geräteumleitung wie vorgesehen funktioniert.

- Bearbeiten Sie die Benutzergeräteregistrierung (oder die INI-Dateien bei Citrix Receiver für Linux). Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Bearbeiten Sie die Administrator-Override-Regeln der VDA-Registrierung auf den Serverbetriebssystemmaschinen. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie VDA über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\vda_usb.adm.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln, wie nachfolgend beschrieben. Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format {Allow:|Deny:} gefolgt von Tag=Wert-Ausdrücken, die durch Leerzeichen getrennt sind. Die folgenden Tags werden unterstützt:

| Tag | Beschreibung |
|---|---|
| VID | Vendor-ID vom Gerätedeskriptor |
| PID | Produkt-ID vom Gerätedeskriptor |
| REL | Release-ID vom Gerätedeskriptor |
| Klasse | Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter http://www.usb.org/. |
| SubClass | Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor |
| Prot | Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor |

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel; Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

> **Important**
>
> Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit Semikolons getrennt eingeben.

Bei optimierten Geräten, wie Massenspeichergeräten, wird das Gerät normalerweise über den speziellen CDM-Kanal umgeleitet und nicht mit Richtlinienregeln. Sie können dieses Verhalten auf die folgende Weise überschreiben:

- Leiten Sie das optimierte Gerät manuell mit der generischen USB-Umleitung um: Wählen Sie im Dialogfeld Einstellungen auf der Registerkarte Geräte die Option Zu allgemein wechseln.
- Leiten Sie das optimierte Gerät automatisch mit der generischen USB-Umleitung um, indem Sie die automatische Umleitung für das Speichergerät festlegen (z. B. AutoRedirectStorage = 1) und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfigurieren. Weitere Informationen finden Sie unter CTX123015.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Vendor- und Produkt-IDs:
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse  Deny: VID=046D # Deny all Logitech products
- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für eine definierte Klasse, Unterklasse und ein Protokoll:
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices  Allow: Class=EF SubClass=01 # Allow Sync devices  Allow: Class=EF # Allow all USB-Miscellaneous devices

### Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen.

Wenn Sie mit Citrix Receiver für Windows arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, werden unmittelbar im USB-Menü von Desktop Viewer angezeigt.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, können Sie das Problem u. U. beheben, indem Sie das Gerät erst nach dem Beginn der virtuellen Sitzung anschließen.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Symbol "Hardware sicher entfernen", bevor Sie das USB-Gerät entfernen.

### USB-Massenspeichergeräte

Nur bei Massenspeichergeräten ist Remotezugriff auch durch Clientlaufwerkszuordnung verfügbar. Hierbei werden Laufwerke auf dem Benutzergerät automatisch Laufwerksbuchstaben auf dem


© 1999-2017 Citrix Systems, Inc. All rights reserved.

virtuellen Desktop zugeordnet, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt. Um Clientlaufwerkzuordnung zu konfigurieren, verwenden Sie unter den ICA-Richtlinieneinstellungen im Abschnitt "Dateiumleitung" die Einstellung Clientwechseldatenträger.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

| Feature | Clientlaufwerkszuordnung | Generische USB-Umleitung |
|---|---|---|
| Diese Option ist in der Standardeinstellung aktiviert. | Ja | Nein |
| Konfigurierbare Leserechte | Ja | Nein |
| Sicheres Entfernen des Geräts in einer Sitzung | Nein | Ja, unter der Voraussetzung, dass Benutzer den Empfehlungen des Betriebssystems zum sicheren Entfernen von Geräten folgen. |

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der Clientlaufwerkzuordnung umgeleitet. Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und für ein Gerät die automatische Umleitung konfiguriert wurde (siehe http://support.citrix.com/article/CTX123015) und wenn ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der generischen USB-Umleitung umgeleitet.

> **Hinweis**
>
> Die USB-Umleitung wird für Verbindungen mit geringer Bandbreite (z. B. 50 KBit/s) unterstützt, das Kopieren großer Dateien funktioniert jedoch nicht.

### Dateizugriff für zugeordnete Clientlaufwerke

Sie können steuern, ob Benutzer Dateien von ihren virtuellen Umgebungen auf ihre Benutzergeräte kopieren können. Standardmäßig ist in der Sitzung Lese-/Schreibzugriff auf Dateien und Ordner auf zugeordneten Clientlaufwerken möglich.

Um zu verhindern, dass Benutzer Dateien und Ordner auf zugeordneten Clientlaufwerken hinzufügen oder ändern, aktivieren Sie die Richtlinieneinstellung Schreibgeschützter Zugriff auf Clientlaufwerke. Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellung Clientlaufwerkumleitung auf Zugelassen festlegen und zur Richtlinie hinzufügen.

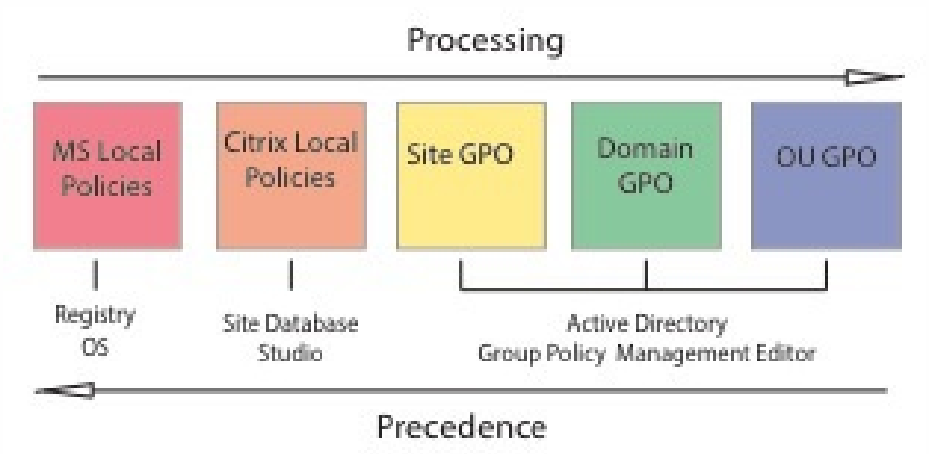

© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Richtlinien

Jul 08, 2016

Richtlinien sind eine Sammlung von Einstellungen, die definieren, wie Sitzungen, Bandbreite und Sicherheit für eine Gruppe von Benutzern, Geräten oder Verbindungstypen verwaltet werden.

Richtlinieneinstellungen können auf physische und virtuelle Maschinen oder auf Benutzer angewendet werden. Sie können Einstellungen auf einzelne Benutzer auf lokaler Ebene oder auf Sicherheitsgruppen in Active Directory anwenden. Die Konfigurationen definieren bestimmten Kriterien und Regeln, und wenn Sie die Richtlinien nicht ausdrücklich zuweisen, gelten die Einstellungen für alle Verbindungen.




Sie können Richtlinien auf unterschiedliche Ebenen des Netzwerks zuweisen. Richtlinieneinstellungen, die auf der GPO-Ebene der Organisationseinheit zugewiesen werden, haben die höchste Priorität im Netzwerk. Richtlinien auf der Domänen-GPO-Ebene überschreiben Richtlinien auf der Ebene der Sitegruppenrichtlinienobjekte, die wiederum alle lokalen Richtlinien von Microsoft und Citrix überschreiben, die mit ihnen in Konflikt stehen.

Alle lokalen Citrix Richtlinien werden in der Citrix Studio-Konsole erstellt und verwaltet und in der Sitedatenbank gespeichert. Gruppenrichtlinien werden hingegen mit der Microsoft-Gruppenrichtlinien-Verwaltungskonsole (GPMC) erstellt und verwaltet und in Active Directory gespeichert. Lokale Microsoft-Richtlinien werden im Windows-Betriebssystem erstellt und in der Registrierung gespeichert.

Studio verwendet einen Modellierungsassistenten, mit dem Administratoren Konfigurationseinstellungen in Vorlagen und Richtlinien vergleichen können, um miteinander in Konflikt stehende und redundante Einstellungen zu eliminieren. Administratoren können Gruppenrichtlinienobjekte mit der Gruppenrichtlinien-Verwaltungskonsole festlegen, um Einstellungen zu konfigurieren und diese Einstellungen auf eine Zielgruppe von Benutzern auf unterschiedlichen Ebenen des Netzwerks anzuwenden.

Diese Gruppenrichtlinienobjekte werden in Active Directory gespeichert und die meisten IT-Mitarbeiter haben aus Sicherheitsgründen nur eingeschränkten Zugriff auf die Verwaltung dieser Einstellungen.

Einstellungen werden entsprechend ihrer Priorität und Bedingung zusammengefasst. Deaktivierte Einstellungen haben Vorrang vor aktivieren Einstellungen mit niedriger Priorität. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

Lokale Richtlinien können auch mit Gruppenrichtlinien in Active Directory in Konflikt stehen. Abhängig von der Situation könnten sie einander überschreiben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Alle Richtlinien werden in der folgenden Reihenfolge verarbeitet:

1. Der Endbenutzer meldet sich mit Domänenanmeldeinformationen an einer Maschine an.
2. Die Anmeldeinformationen werden an den Domänencontroller gesendet.
3. Active Directory wendet alle Richtlinien an (Endbenutzer, Endpunk, Organisationseinheit und Domäne).
4. Der Endbenutzer meldet sich bei Receiver an und greift auf eine Anwendung oder einen Desktop zu.
5. Richtlinien von Citrix und Microsoft werden für den Endbenutzer und die Maschine, die die Ressource hostet, verarbeitet.
6. Active Directory bestimmt die Priorität für die Richtlinieneinstellungen und wendet sie auf die Registrierung des Endpunktgeräts und die Maschine an, auf der die Ressource gehostet wird.
7. Der Endbenutzer meldet sich von der Ressource ab. Citrix Richtlinien für Endbenutzer und Endpunktgerät sind nicht mehr aktiv.
8. Der Endbenutzer meldet sich vom Benutzergerät ab, das die GPO-Benutzerrichtlinien freigibt.
9. Der Endbenutzer schaltet das Gerät aus und die GPO-Maschinenrichtlinien werden freigegeben.

Beim Erstellen von Richtlinien für Benutzergruppen, Geräte und Maschinen haben einige Mitglieder u. U. unterschiedliche Anforderungen und benötigen Ausnahmen zu einigen Einstellungen. Ausnahmen werden durch Filter in Studio und in der Gruppenrichtlinien-Verwaltungskonsole erstellt und bestimmten, für wen oder was die Richtlinie gilt.

**Hinweis:** Die Verwendung von Windows- und Citrix Richtlinien im gleichen GPO wird nicht unterstützt.

## Verwandter Inhalt

- Arbeiten mit Richtlinien
- Richtlinienvorlagen
- Erstellen von Richtlinien
- Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien
- Standardrichtlinieneinstellungen
- Referenz für Richtlinieneinstellungen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Arbeiten mit Richtlinien

Jul 08, 2016

Durch das Konfigurieren von Citrix Richtlinien steuern Sie den Benutzerzugriff und die Sitzungsumgebung. Citrix Richtlinien sind die effizienteste Methode zum Steuern der Verbindungs-, Sicherheits- und Bandbreiteneinstellungen. Sie erstellen Richtlinien für bestimmte Benutzergruppen, Geräte oder Verbindungstypen. Jede Richtlinie kann mehrere Einstellungen enthalten.

## Tools zum Arbeiten mit Citrix Richtlinien

Sie können die folgenden Tools zum Arbeiten mit Citrix Richtlinien verwenden.

- **Studio**: Wenn Sie ein Citrix Administrator ohne Berechtigung zum Verwalten von Gruppenrichtlinien sind, verwenden Sie Studio, um Richtlinien für Ihre Site zu erstellen. Mit Studio erstellte Richtlinien werden in der Sitedatenbank gespeichert und Updates werden per Push auf den virtuellen Desktop übertragen, wenn der virtuelle Desktop beim Broker registriert wird oder ein Benutzer eine Verbindung mit dem virtuellen Desktop herstellt.
- **Editor für lokale Gruppenrichtlinien** (Snap-In der Microsoft Management Console): Wenn Sie in Ihrer Netzwerkumgebung Active Directory verwenden und Sie die Berechtigungen zur Verwaltung von Gruppenrichtlinien haben, können Sie den Editor für lokale Gruppenrichtlinien verwenden, um Richtlinien für Ihre Site zu erstellen. Die Einstellungen, die Sie konfigurieren, beeinträchtigen die Gruppenrichtlinienobjekte, die Sie in der Gruppenrichtlinien-Verwaltungskonsole angeben.
  Wichtig: Sie müssen den Editor für lokale Gruppenrichtlinien zum Konfigurieren einiger Einstellungen verwenden, u. a. die Einstellungen zum Registrieren von VDAs bei einem Controller und die Einstellungen für Microsoft App-V Server.

## Reihenfolge und Priorität bei der Richtlinienverarbeitung

Gruppenrichtlinieneinstellungen (GPOs) werden in der folgenden Reihenfolge verarbeitet:

1. Lokale GPO
2. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)
3. GPOs auf Siteebene
4. GPOs auf Domänenebene
5. Organisationseinheiten

Bei einem Konflikt können Richtlinieneinstellungen, die zuletzt verarbeitet werden, vorher verarbeitete überschreiben. Das heißt, dass Richtlinieneinstellungen die folgende Rangfolge haben:

1. Organisationseinheiten
2. GPOs auf Domänenebene
3. GPOs auf Siteebene
4. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)
5. Lokale GPO

Beispiel: Ein Citrix Administrator erstellt eine Richtlinie (Richtlinie A) über Studio, mit der die Clientdateiumleitung für die Vertriebsmitarbeiter des Unternehmens aktiviert wird. Gleichzeitig erstellt ein anderer Administrator mit dem Gruppenrichtlinien-Editor eine Richtlinie (Richtlinie B), mit der die Clientdateiumleitung für die Vertriebsmitarbeiter deaktiviert wird. Wenn sich die Vertriebsmitarbeiter an den virtuellen Desktops anmelden, wird Richtlinie B angewendet und Richtlinie A ignoriert, da Richtlinie B auf der Domänenebene und Richtlinie A auf der Ebene der XenApp- bzw. XenDesktop-Site-GPOs verarbeitet wurde.

Beachten Sie jedoch, dass die Citrix Sitzungseinstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder


© 1999-2017 Citrix Systems, Inc. All rights reserved.

einer Remotedesktop-Sitzungshostkonfiguration überschreiben, wenn ein Benutzer eine ICA- oder Remotedesktopprotokoll (RDP)-Sitzung startet. Zu diesen Einstellungen gehören solche, die mit typischen RDP-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimationen und das Anzeigeverhalten bei Drag & Drop.

Wenn Sie mehrere Richtlinien verwenden, können Sie Richtlinien, deren Einstellungen Konflikte verursachen, Prioritäten zuweisen. Weitere Informationen hierzu finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

## Arbeitsablauf bei Citrix Richtlinien

Der Prozess für das Konfigurieren von Richtlinien ist:

1. Erstellen Sie die Richtlinie.
2. Konfigurieren Sie Richtlinieneinstellungen.
3. Weisen Sie die Richtlinie Benutzer- und Maschinenobjekten zu.
4. Weisen Sie der Richtlinie eine Priorität zu.
5. Prüfen Sie die effektive Richtlinie durch Ausführen des Gruppenrichtlinien-Modellierungsassistenten.

## Navigieren durch die Citrix Richtlinien und Einstellungen

Im Editor für lokale Gruppenrichtlinien werden Richtlinien und Einstellungen in zwei Hauptkategorien eingeteilt: Computerkonfiguration und Benutzerkonfiguration. Jede Kategorie hat einen Knoten für Citrix Richtlinien. Weitere Informationen zum Verwenden dieses Snap-Ins finden Sie in der Dokumentation von Microsoft.

In Studio sind die Richtlinieneinstellungen je nach Funktionalität bzw. Feature, für die bzw. das sie gelten, in Kategorien eingeteilt. Beispielsweise enthält der Bereich "Profilverwaltung" Richtlinieneinstellungen für die Profilverwaltung.

- Computereinstellungen (Richtlinieneinstellungen für Maschinen) definieren das Verhalten von virtuellen Desktops und werden beim Start eines virtuellen Desktops angewendet. Diese Einstellungen werden auch angewendet, wenn keine aktiven Benutzersitzungen auf dem virtuellen Desktop durchgeführt werden. Benutzerrichtlinieneinstellungen definieren die Benutzererfahrung bei Verbindungen über ICA. Benutzerrichtlinien werden angewendet, wenn ein Benutzer eine Verbindung über ICA herstellt oder erneut herstellt. Benutzerrichtlinien werden nicht angewendet, wenn ein Benutzer eine Verbindung über RDP herstellt oder sich direkt bei der Konsole anmeldet.
  Sie greifen auf Richtlinien, Einstellungen oder Vorlagen zu, indem Sie im Navigationsbereich von Studio Richtlinien auswählen.
  - Die Registerkarte **Richtlinien** listet alle Richtlinien auf. Wenn Sie eine Richtlinie auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Übersicht (Name, Priorität, Status: Aktiviert bzw. Deaktiviert, und Beschreibung), Einstellungen (Liste der konfigurierten Einstellungen) und Zugewiesen zu (Benutzer- und Maschinenobjekte, denen die Richtlinie momentan zugewiesen ist). Weitere Informationen finden Sie unter Erstellen von Richtlinien.
  - Auf der Registerkarte **Vorlagen** werden von Citrix bereitgestellte und benutzerdefinierte Vorlagen, die Sie erstellt haben, aufgelistet. Wenn Sie eine Vorlage auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Beschreibung (Zweck der Vorlage) und Einstellungen (Liste der konfigurierten Einstellungen). Weitere Informationen finden Sie unter Richtlinienvorlagen.
  - Mit der Registerkarte **Vergleich** können Sie die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.
  - Auf der Registerkarte **Modellierung** können Sie Verbindungsszenarios mit Citrix Richtlinien simulieren. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

  Suchen nach einer Einstellung in einer Richtlinie oder Vorlage


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie die Richtlinie oder Vorlage aus.
2. Wählen Sie im Aktionsbereich Richtlinie bearbeiten oder Vorlage bearbeiten.
3. Geben Sie auf der Seite Einstellungen den Namen der Einstellung ein.

   Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie (z. B. Bandbreite) auswählen oder indem Sie das Kontrollkästchen Nur ausgewählte anzeigen aktivieren. Außerdem können Sie nur die Einstellungen suchen, die der ausgewählten Richtlinie hinzugefügt wurden. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

- Suchen nach einer Einstellung in einer Richtlinie
  1. Markieren Sie die Richtlinie.
  2. Geben Sie auf der Registerkarte Einstellungen den Namen der Einstellung ein.

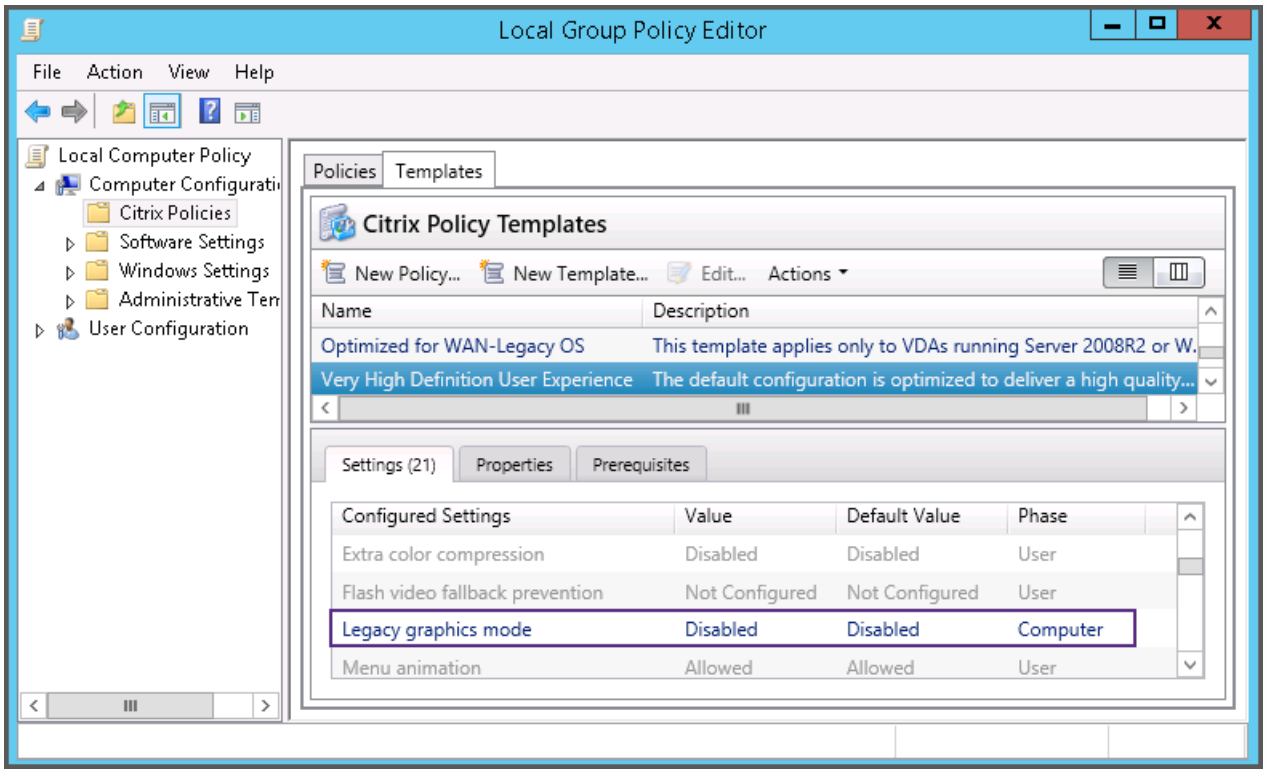
Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie auswählen. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

Eine Richtlinie ist nach ihrer Erstellung völlig unabhängig von der verwendeten Vorlage. Sie können in das Feld "Beschreibung" eingeben, auf welcher Vorlage die neue Richtlinie basiert.

In Studio werden Richtlinien und Vorlagen in einer Liste angezeigt, unabhängig davon, ob sie Benutzer- oder Computereinstellungen oder beide Arten von Einstellungen enthalten, und sie können zudem mit Benutzer- und Computerfiltern angewendet werden.

Im Gruppenrichtlinien-Editor müssen Computer- und Benutzereinstellungen separat angewendet werden, selbst wenn sie auf einer Vorlage basieren, die beide Arten von Einstellungen enthält. In diesem Beispiel wird "Besonders gute High Definition-Benutzererfahrung" in Computerkonfiguration verwendet:

- Der Legacy-Grafikmodus ist eine Computereinstellung, die in einer mit dieser Vorlage erstellten Richtlinie verwendet wird.
- Die Benutzereinstellungen, grau dargestellt, werden nicht in einer mit dieser Vorlage erstellten Richtlinie verwendet.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Richtlinienvorlagen

Jul 08, 2016

Vorlagen ermöglichen das Erstellen von Richtlinien von einem vordefinierten Ausgangspunkt aus. Integrierte Citrix Vorlagen sind für bestimmte Umgebungen oder Netzwerkbedingungen optimiert und können für Folgendes verwendet werden:

- Als Ausgangspunkt für das Erstellen Ihrer eigenen Richtlinien und Vorlagen, die Sie für verschiedene Sites freigeben können.
- Eine Referenz für einfacheres Vergleichen der Ergebnisse zwischen Bereitstellungen, da Sie sich auf Ergebnisse beziehen können, zum Beispiel "... wenn Sie die Citrix Vorlage x oder y verwenden ...".
- Eine Methode für das Übermitteln von Richtlinien an Citrix Support oder vertrauenswürdige Dritte durch Importieren oder Exportieren von Vorlagen.

Richtlinienvorlagen können importiert und exportiert werden. Weitere Vorlagen und/oder Updates für die integrierten Vorlagen finden Sie unter CTX202000.

Informationen zur Verwendung von Vorlagen für die Erstellung von Richtlinien finden Sie unter CTX202330.

## Integrierte Citrix Vorlagen

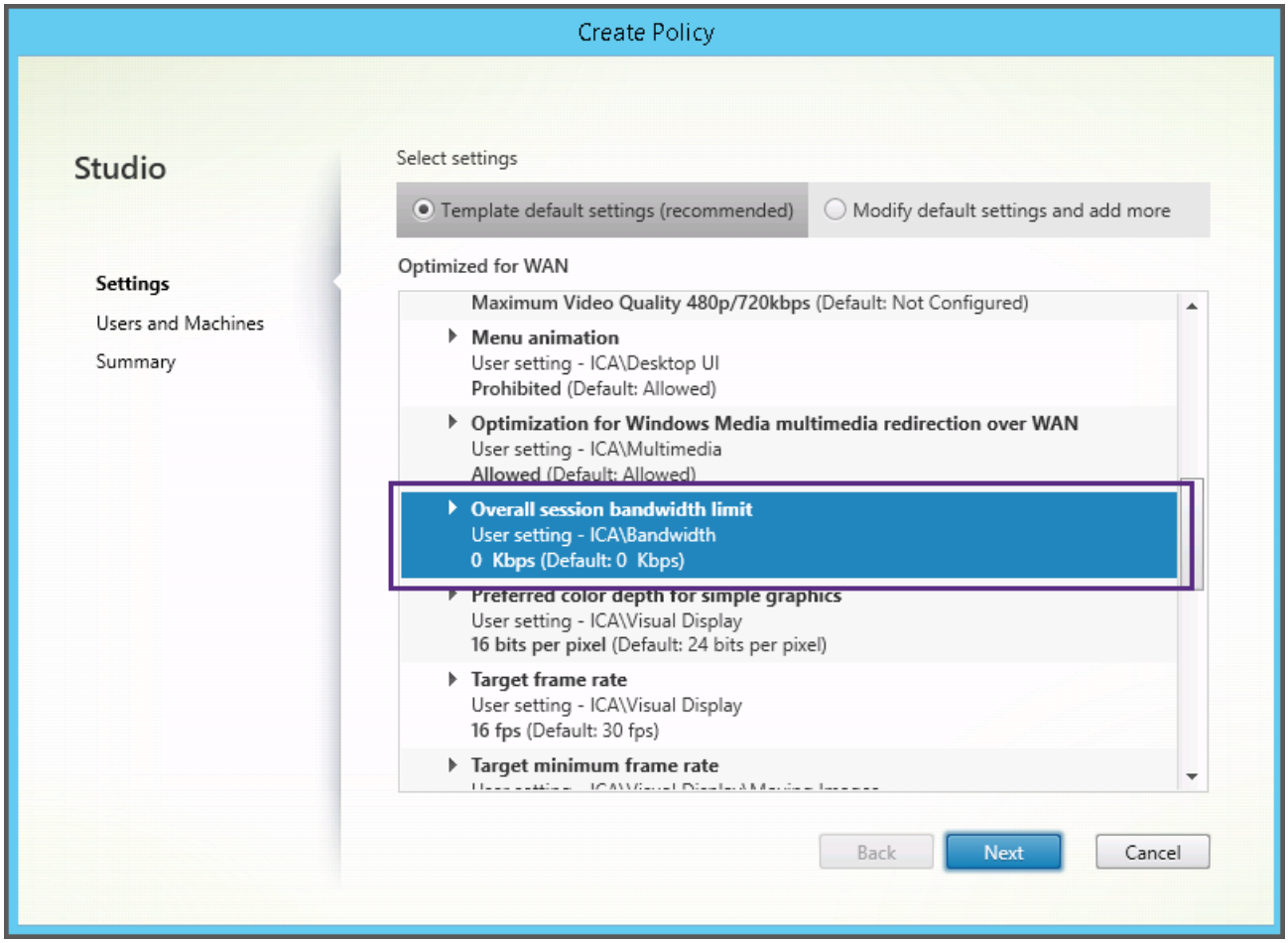
Die folgenden Richtlinienvorlagen sind verfügbar:

- **Besonders gute High Definition-Benutzererfahrung**: Diese Vorlage erzwingt die Standardeinstellungen zum Optimieren der Benutzererfahrung. Verwenden Sie diese Vorlage in Szenarios, in denen mehrere Richtlinien in der Reihenfolge der Priorität verarbeitet werden.
- **Hohe Serverskalierbarkeit**: Mit dieser Vorlage können Sie Serverressourcen sparen, da Benutzererfahrung und Serverskalierbarkeit ausbalanciert werden. Die Vorlage ermöglicht eine gute Benutzererfahrung und erhöht gleichzeitig die Anzahl an Benutzern, die auf einem einzelnen Server gehostet werden können. Diese Vorlage verwendet keinen Videocodec für die Komprimierung von Grafiken und verhindert das serverseitige Multimediarendering.
- **Hohe Serverskalierbarkeit – Legacy-OS**: Diese Vorlage für hohe Serverskalierbarkeit gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 und älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Für WAN optimiert**: Verwenden Sie diese Vorlage bei aufgabenorientierten Mitarbeitern, die in Geschäftsstellen über eine gemeinsam genutzte WAN-Verbindung arbeiten oder bei Remotestandorten, wo über Verbindungen mit geringer Bandbreite auf Anwendungen mit grafisch einfachen Benutzeroberflächen und wenig Multimediainhalt zugegriffen wird. Mit dieser Vorlage werden für optimierte Bandbreiteneffizienz Kompromisse bei der Qualität der Videowiedergabe und der Serverskalierbarkeit gemacht.
- **Für WAN optimiert – Legacy-OS**: Diese Vorlage gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 oder älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Sicherheit und Steuerung**: Verwenden Sie diese Vorlage in Umgebungen mit niedriger Fehlertoleranz, um die in XenApp und XenDesktop standardmäßig aktivierten Features zu minimieren. Die in dieser Vorlage enthaltenen Einstellungen deaktivieren den Zugriff auf Drucker, Zwischenablage, Peripheriegeräte, Laufwerkzuordnung, Portumleitung und Flash-Beschleunigung auf Benutzergeräten. Bei Anwendung dieser Vorlage wird möglicherweise mehr Bandbreite genutzt und die Benutzerdichte pro Server verringert.

Wir empfehlen zwar, die integrierten Citrix Vorlagen mit den Standardeinstellungen zu verwenden, jedoch haben einige Einstellungen keine empfohlenen Werte (z. B. die Einstellung "Bandbreitenlimit für Sitzung insgesamt" in der Vorlage "Für


© 1999-2017 Citrix Systems, Inc. All rights reserved.

WAN optimiert"). In diesem Fall wird die Einstellung durch die Vorlage verfügbar gemacht, damit der Administrator die Wirkung dieser Einstellung in diesem Szenario versteht.




Wenn Sie eine Bereitstellung (Richtlinienverwaltung und VDAs) vor XenApp und XenDesktop 7.6 FP3 betreiben und die Vorlagen "Hohe Serverskalierbarkeit" und "Für WAN optimiert" benötigen, verwenden Sie die Vorlagenversionen für ältere Betriebssysteme ("Legacy-OS").

> **Hinweis**
>
> Integrierte Vorlagen werden von Citrix erstellt und aktualisiert. Diese Vorlagen dürfen nicht geändert oder gelöscht werden.

## Erstellen und Verwalten von Vorlagen mit Studio

Erstellen einer neuen Vorlage basierend auf einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie eine neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Vorlage erstellen**.
4. Wählen und konfigurieren Sie die Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen für die Vorlage ein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird die neue Vorlage auf der Registerkarte **Vorlagen** angezeigt.

Erstellen einer neuen Vorlage basierend auf einer Richtlinie

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Als Vorlage speichern**.
4. Wählen und konfigurieren Sie die neuen Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

Importieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage importieren**.
3. Wählen Sie die Vorlagendatei, die Sie importieren möchten, und klicken Sie auf **Öffnen**. Wenn Sie eine Vorlage importieren, die denselben Namen wie eine vorhandene hat, können Sie die vorhandene Vorlage überschreiben oder die Vorlage unter einem anderen Namen speichern, der automatisch generiert wird.

Exportieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage exportieren**.
3. Legen Sie den Speicherort für die Vorlage fest, und klicken Sie auf **Speichern**.

Im angegebenen Speicherort wird eine GPT-Datei erstellt.

## Erstellen und Verwalten von Vorlagen mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration oder Benutzerkonfiguration. Erweitern Sie den Knoten Richtlinien und wählen Sie dann Citrix Richtlinien. Wählen Sie die entsprechende Aktion aus.

| Aufgabe | Anweisung |
|---|---|
| Erstellen einer Vorlage basierend auf einer vorhandenen Richtlinie | Wählen Sie auf der Registerkarte "Richtlinien" die Richtlinie aus, und wählen Sie dann Aktionen > Als Vorlage speichern. |
| Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie. |
| Erstellen einer Vorlage basierend auf einer vorhandenen Vorlage | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Vorlage. |
| Importieren einer Vorlage | Wählen Sie auf die Registerkarte "Vorlagen" die Optionen Aktionen > Importieren. |
| Exportieren einer Vorlage | Wählen Sie auf die Registerkarte "Vorlagen" die Optionen Aktionen > Exportieren. |
| Anzeigen der Vorlageneinstellungen | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Einstellungen". |
| | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Aufgabe | Anweisung |
| --- | --- |
| Anzeigen einer Zusammenfassung von Vorlageneigenschaften | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Eigenschaften". |
| Anzeigen von Vorlagenvoraussetzungen | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Voraussetzungen". |

## Vorlagen und delegierte Administration

Richtlinienvorlagen werden auf der Maschine gespeichert, auf der das Richtlinienverwaltungspaket installiert wurde. Das ist entweder die Maschine mit dem Delivery Controller oder die Maschine für die Verwaltung der Gruppenrichtlinienobjekte, jedoch nicht die Maschine mit der XenApp- und XenDesktop-Sitedatenbank. Daher werden die Richtlinienvorlagen nicht über die Rollen und Geltungsbereiche der delegierten Site-Verwaltung, sondern über Windows-Administratorrechte gesteuert.

Dies bedeutet, dass ein Administrator, der über Leseberechtigungen für die Site verfügt, beispielsweise neue Vorlagen erstellen kann. Da Vorlagen jedoch lokale Dateien sind, werden an der Umgebung keine Änderungen vorgenommen.

Benutzerdefinierte Vorlagen sind für das Benutzerkonto sichtbar, das sie erstellt hat, und werden im Windows-Profil des Benutzers gespeichert. Wenn Sie eine benutzerdefinierte Vorlage umfassender verfügbar machen möchten, erstellen Sie daraus eine Richtlinie oder exportieren Sie die Vorlage in einen freigegebenen Speicherort.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen von Richtlinien

Jul 08, 2016

Legen Sie vor dem Erstellen einer Richtlinie fest, für welche Benutzergruppen oder Geräte sie gelten soll. Sie können Richtlinien basierend auf Aufgabenbereich, Verbindungstyp, Benutzergerät oder geografischer Position erstellen. Alternativ können Sie die gleichen Kriterien verwenden wie für Windows Active Directory-Gruppenrichtlinien.

Wenn Sie bereits eine Richtlinie für eine Gruppe erstellt haben, sollten Sie möglichst die Richtlinie bearbeiten und die entsprechenden Einstellungen konfigurieren, statt eine andere Richtlinie zu erstellen. Vermeiden Sie es, eine neue Richtlinie zu erstellen, deren einziger Zweck ist, eine bestimmte Einstellung zu aktivieren oder bestimmte Benutzer von der Richtlinie auszunehmen.

Wenn Sie eine Richtlinie erstellen, verwenden Sie als Basis eine Richtlinienvorlage und passen Sie die Einstellungen nach Bedarf an. Sie können die Richtlinie natürlich auch ohne Vorlage erstellen und alle benötigten Einstellungen hinzufügen.

## Richtlinieneinstellungen

Richtlinieneinstellungen können deaktiviert, aktiviert oder nicht konfiguriert sein. Standardmäßig sind Richtlinieneinstellungen nicht konfiguriert, d. h. sie wurden keiner Richtlinie hinzugefügt. Einstellungen werden nur angewendet, wenn sie einer Richtlinie hinzugefügt wurden.

Manche Richtlinieneinstellungen können einen der folgenden Zustände haben:

- Mit Zugelassen oder Nicht zugelassen wird die durch die Einstellung gesteuerte Aktion ermöglicht oder verhindert. In manchen Fällen dürfen Benutzer die Aktion der Einstellung in der Sitzung verwalten, in anderen dürfen sie das nicht. Wenn beispielsweise für Menüanimation die Einstellung auf "Zugelassen" festgelegt ist, können Benutzer Menüanimationen in ihrer Clientumgebung steuern.
- Mit Aktiviert oder Deaktiviert schalten Sie die Einstellung ein oder aus. Wenn Sie eine Einstellung deaktivieren, wird sie nicht durch Richtlinien mit geringerer Priorität aktiviert.

Manche Einstellungen steuern außerdem die Wirksamkeit von abhängigen Einstellungen. Die Einstellung Clientlaufwerkumleitung steuert beispielsweise, ob Benutzer auf die Laufwerke ihres Geräts zugreifen können. Damit Benutzer auf Netzlaufwerke zugreifen können, muss sowohl diese Einstellung als auch die Einstellung Clientnetzlaufwerke der Richtlinie hinzugefügt werden. Wenn die Einstellung Clientlaufwerkumleitung deaktiviert ist, können Benutzer nicht auf ihre Netzlaufwerke zugreifen, selbst wenn die Einstellung Clientnetzlaufwerke aktiviert ist.

In der Regel treten Änderungen an Richtlinieneinstellungen, die sich auf Maschinen auswirken, in Kraft, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet. Änderungen an Richtlinieneinstellungen, die Auswirkungen auf Benutzer haben, treten in Kraft, wenn sich die Benutzer das nächste Mal anmelden. Wenn Sie Active Directory verwenden, werden die Richtlinieneinstellungen aktualisiert, wenn Active Directory die Richtlinien in 90-Minuten-Intervallen erneut evaluiert. Die Richtlinieneinstellungen werden angewendet, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet.

Für manche Richtlinieneinstellungen können Sie einen Wert eingeben oder auswählen, wenn Sie die Einstellung der Richtlinie hinzufügen. Sie können die Konfiguration der Einstellung einschränken, indem Sie Standardwert verwenden wählen. Dadurch deaktivieren Sie die Konfiguration der Einstellung und nur der Standardwert der Einstellung darf verwendet werden, wenn die Richtlinie angewendet wird, unabhängig von dem Wert, der vor dem Aktivieren von Standardwert verwenden eingegeben wurde.

Bewährte Methoden:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Weisen Sie Richtlinien Gruppen statt einzelnen Benutzern zu. Wenn Sie Richtlinien Gruppen zuweisen, werden Zuweisungen automatisch aktualisiert, wenn Sie Benutzer Gruppen hinzufügen oder sie daraus entfernen.
- Aktivieren Sie nicht widersprechende oder überlappende Einstellungen in der Konfiguration des Remotedesktop-Sitzungshosts. In manchen Fällen bietet die Remotedesktop-Sitzungshostkonfiguration ähnliche Funktionalität wie Citrix Richtlinieneinstellungen. Wählen Sie nach Möglichkeit für alle Einstellungen den gleichen Status (aktiviert oder deaktiviert), um die Problembehandlung zu erleichtern.
- Deaktivieren Sie Richtlinien, die nicht verwendet werden. Richtlinien, denen keine Einstellungen hinzugefügt wurden, verursachen unnötigen Verarbeitungsaufwand.

## Richtlinienzuweisungen

Wenn Sie eine Richtlinie erstellen und bestimmten Benutzer- und Maschinenobjekten zuweisen, wird sie gemäß bestimmter Kriterien oder Regeln auf Verbindungen angewendet. Basierend auf einer Kombination von Kriterien können Sie in der Regel beliebig viele Zuweisungen für eine Richtlinie hinzufügen. Wenn keine Zuweisung angegeben wurde, gilt die Richtlinie für alle Verbindungen.

In der folgenden Tabelle werden verfügbare Zuweisungen aufgelistet:

| Name | Anwendung der Richtlinie basierend auf |
|---|---|
| Zugriffssteuerung | Zugriffssteuerungsbedingungen, unter denen Clients eine Verbindung herstellen<br>• Verbindungstyp: Ob die Richtlinie auf Verbindungen anzuwenden ist, die mit oder ohne NetScaler Gateway hergestellt wurden.<br>• NetScaler Gateway-Farmname: Name des virtuellen NetScaler Gateway-Servers.<br>• Zugriffsbedingung: Name der zu verwendenden Endpunktanalyserichtlinie oder Sitzungsrichtlinie. |
| Citrix CloudBridge | Ob eine Benutzersitzung über Citrix CloudBridge gestartet wird.<br><br>Hinweis: Sie können einer Richtlinie nur eine Citrix CloudBridge-Zuweisung hinzufügen. |
| Client-IP-Adresse | IP-Adresse des Benutzergeräts, das zum Verbinden der Sitzung verwendet wird<br>• IPv4-Beispiele: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24<br>• IPv6-Beispiele: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Clientname | Name des Benutzergeräts<br><br>• Genaue Übereinstimmung: ClientABCName<br>• Verwenden von Platzhalter: Client*Name |
| Bereitstellungsgruppe | Bereitstellungsgruppen-Mitgliedschaft |
| Bereitstellungsgruppentyp | Desktop- oder Anwendungstyp: privater Desktop, freigegebener Desktop, private Anwendung oder freigegebene Anwendung |
| Organisationseinheit | Organisationseinheit |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Tag<br>Name | Tags<br>Anwendung der Richtlinie basierend auf |
|---|---|
| | **Hinweis:** Installieren Sie den unter CTX142439 verfügbaren Hotfix, um sicherzustellen, dass die Richtlinien bei der Verwendung von Tags richtig angewendet werden. |
| Benutzer oder Gruppe | Benutzer- oder Gruppenname |

Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet. Jede deaktivierte Richtlinieneinstellung hat Vorrang vor einer aktivierten Richtlinieneinstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert.

Wichtig: Bei der Konfiguration von Active Directory- und Citrix Richtlinien mit der Gruppenrichtlinien-Verwaltungskonsole werden Zuweisungen und Einstellungen möglicherweise nicht wie erwartet angewendet. Weitere Informationen finden Sie unter CTX127461.
Eine Richtlinie mit dem Namen "Ungefiltert" ist standardmäßig verfügbar.

- Wenn Sie Studio zur Verwaltung von Citrix Richtlinien verwenden, werden die Einstellungen, die Sie der Richtlinie "Ungefiltert" hinzufügen, auf alle Server, Desktops und Verbindungen einer Site angewendet.
- Wenn Sie mit dem Editor für lokale Gruppenrichtlinien Citrix Richtlinien verwalten, gelten Einstellungen, die Sie der Richtlinie "Ungefiltert" hinzufügen, für alle Sites und Verbindungen, die zu dem Geltungsbereich des Gruppenrichtlinienobjekts gehören, das die Richtlinie enthält. Beispiel: Die Organisationseinheit (OU) "Verkauf" enthält ein Gruppenrichtlinienobjekt "Verkauf-USA", das alle Mitarbeiter des US-Verkaufsteams einschließt. Das Gruppenrichtlinienobjekt "Verkauf-USA" ist mit einer Richtlinie "Ungefiltert" konfiguriert, die mehrere Benutzerrichtlinieneinstellungen enthält. Wenn der US-Verkaufsleiter sich an der Site anmeldet, werden die Einstellungen der Richtlinie "Ungefiltert" automatisch auf die Sitzung angewendet, weil der Benutzer Mitglied des Gruppenrichtlinienobjekts "Verkauf-USA" ist.

Der Modus einer Zuweisung entscheidet, ob die Richtlinie nur auf Verbindungen angewendet wird, die alle Zuweisungskriterien erfüllen. Wenn der Modus Zulassen (Standardwert) ist, wird die Richtlinie nur auf Verbindungen angewendet, die die Zuweisungskriterien erfüllen. Wenn der Modus Verweigern ist, wird die Richtlinie angewendet, wenn eine Verbindung die Zuweisungskriterien nicht erfüllt. Das folgende Beispiel zeigt, wie Zuweisungsmodi sich auf Citrix Richtlinien auswirken, wenn mehrere Zuweisungen vorhanden sind.

- **Beispiel: Zuweisungen des gleichen Typs mit unterschiedlichen Modi**: In Richtlinien mit zwei Zuweisungen des gleichen Typs, eine mit der Einstellung Zulassen und die andere mit der Einstellung Verweigern, hat die Zuweisung mit der Einstellung Verweigern Vorrang, wenn die Verbindung die Kriterien beider Zuweisungen erfüllt. Beispiel:
  Richtlinie 1 enthält die folgenden Zuweisungen:
  - Zuweisung A bestimmt die Verkaufsgruppe, und der Modus ist Zulassen
  - Zuweisung B bestimmt das Konto des Verkaufsleiters, und der Modus ist Verweigern

  Da der Modus für Zuweisung B Verweigern ist, wird die Richtlinie nicht angewendet, wenn der Verkaufsleiter sich bei der Site anmeldet, obwohl er Mitglied der Verkaufsgruppe ist.

- **Beispiel: Zuweisungen unterschiedlichen Typs mit gleichen Modi**: In Richtlinien mit zwei oder mehr Zuweisungen unterschiedlichen Typs, für die Zulassen eingestellt ist, muss die Verbindung die Kriterien von mindestens einer Zuweisung jedes Typs erfüllen, damit die Richtlinie angewendet wird. Beispiel:
  Richtlinie 2 enthält die folgenden Zuweisungen:
  - Zuweisung C ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Zuweisung D ist eine Client-IP-Adressenzuweisung, die 10.8.169.* festlegt (das Unternehmensnetzwerk), und der Modus ist Zulassen.

Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie angewendet, weil die Verbindung die Kriterien beider Zuweisungen erfüllt.

Richtlinie 3 enthält die folgenden Zuweisungen:

- Zuweisung E ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen
- Zuweisung F ist eine Zugriffssteuerungszuweisung, die NetScaler Gateway-Verbindungsbedingungen angibt, und der Modus ist Zulassen.

Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie nicht angewendet, weil die Verbindung nicht die Kriterien von Zuweisung F erfüllt.

### Erstellen einer Richtlinie basierend auf einer Vorlage mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte "Vorlagen" und wählen Sie dann eine Vorlage.
3. Wählen Sie im Aktionsbereich Richtlinie aus Vorlage erstellen.
4. Standardmäßig verwendet die neue Richtlinie alle Standardeinstellungen der Vorlage (das Optionsfeld Standardeinstellungen der Vorlage ist ausgewählt). Um die Einstellungen zu ändern, wählen Sie das Optionsfeld Standardeinstellungen ändern und Einstellungen hinzufügen, und fügen Sie Einstellungen hinzu oder entfernen Sie sie.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:
   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.
   - Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.
6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.
   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

### Erstellen einer Richtlinie mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte Richtlinien.
3. Wählen Sie im Aktionsbereich Richtlinie erstellen.
4. Fügen Sie Richtlinieneinstellungen nach Bedarf hinzu und konfigurieren Sie diese.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:
   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.
   - Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.
6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.
   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

### Erstellen und Verwalten von Richtlinien mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration oder Benutzerkonfiguration. Erweitern Sie den Knoten Richtlinien und wählen Sie dann Citrix Richtlinien. Wählen Sie die entsprechende Aktion aus.

| Aufgabe | Anweisung |
|---|---|
| Erstellen einer Richtlinie | Klicken Sie auf der Registerkarte "Richtlinien" auf Neu. |
| Bearbeiten einer bestehenden Richtlinie | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Bearbeiten. |
| Ändern der Priorität einer bestehenden Richtlinie | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Höhere Priorität oder Geringere Priorität. |
| Anzeigen einer Zusammenfassung über eine Richtlinie | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Zusammenfassung. |
| Anzeigen und Ändern der Richtlinieneinstellungen | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Einstellungen. |
| Anzeigen und Ändern der Richtlinienfilter | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Einstellungen. |
| Aktivieren oder Deaktivieren einer Richtlinie | Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Aktionen > Aktivieren oder Aktionen > Deaktivieren. |
| Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage | Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien

Jul 08, 2016

Sie können mit mehreren Richtlinien Ihre Umgebung an die Anforderungen der Benutzer, basierend auf deren Aufgabengebiet, geografischem Standort oder Verbindungstyp anpassen. Beispielsweise sind Sie vielleicht aus Sicherheitsgründen gezwungen, Benutzergruppen, die regelmäßig mit sensiblen Daten arbeiten, Beschränkungen aufzuerlegen. Sie können eine Richtlinie erstellen, die Benutzer daran hindert, vertrauliche Daten auf ihren lokalen Clientlaufwerken zu speichern. Wenn jedoch manche Mitglieder dieser Benutzergruppe Zugang zu ihren lokalen Laufwerken benötigen, können Sie eine andere Richtlinie für diese Benutzer erstellen. Anschließend können Sie den beiden Richtlinien jeweils eine Priorität zuweisen und damit festlegen, welche Richtlinie Vorrang haben soll.

Wenn Sie mehrere Richtlinien verwenden, müssen Sie festlegen, wie Prioritäten zugewiesen und Ausnahmen erstellt werden und wie die wirksame Richtlinie bei Richtlinienkonflikten angezeigt wird.

In der Regel setzen Richtlinien ähnliche Einstellungen, die für die gesamte Site, für bestimmte Delivery Controller oder auf dem Benutzergerät konfiguriert wurden, außer Kraft. Die Ausnahme von diesem Prinzip sind Sicherheitseinstellungen. Die höchste Verschlüsselungseinstellung in der Umgebung, einschließlich Betriebssystem, und die Spiegelungseinstellung mit der größten Einschränkung haben immer Vorrang vor allen anderen Einstellungen und Richtlinien.

Citrix Richtlinien interagieren mit den Richtlinien, die Sie im Betriebssystem eingestellt haben. In einer Citrix Umgebung überschreiben Citrix Einstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder in der Konfiguration des Remotedesktop-Sitzungshosts. Dazu gehören auch Einstellungen, die mit typischen Remotedesktopprotokoll-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimation und das Anzeigeverhalten beim Drag & Drop. Manche Richtlinieneinstellungen, wie SecureICA, müssen mit den Richtlinien und Einstellungen im Betriebssystem übereinstimmen. Wenn anderswo ein höherer Verschlüsselungsgrad festgelegt wurde, kann die SecureICA-Richtlinieneinstellung oder die Einstellung beim Veröffentlichen einer Anwendung außer Kraft gesetzt werden.

Die beim Erstellen von Bereitstellungsgruppen angegebenen Verschlüsselungseinstellungen sollten beispielsweise den gleichen Verschlüsselungsgrad verwenden, den Sie an anderer Stelle in der Umgebung verwenden.

Hinweis: Wenn im zweiten Hop eines Double-Hop-Szenarios ein Desktopbetriebssystem-VDA eine Verbindung mit einem Serverbetriebssystem-VDA herstellt, ist die Wirkung der Citrix Richtlinien auf den Desktopbetriebssystem-VDA die gleiche wie beim Benutzergerät. Wenn Richtlinien beispielsweise das Zwischenspeichern von Bildern auf dem Benutzergerät festlegen, werden die Bilder, die während des zweiten Hop in einem Double-Hop-Szenario zwischengespeichert werden, auf der Desktopbetriebssystem-VDA-Maschine zwischengespeichert.

## Vergleichen von Richtlinien und Vorlagen

Sie können die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Außerdem ist ggf. ein Vergleich von Einstellungen in einer Richtlinie oder Vorlage mit den Standardeinstellungen von Citrix erforderlich.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Klicken Sie auf die Registerkarte "Vergleich" und dann auf Auswählen.
3. Wählen Sie die Richtlinien oder Vorlagen aus, die Sie vergleichen möchten. Aktivieren Sie das Kontrollkästchen Mit Standardeinstellungen vergleichen, um Standardwerte im Vergleich einzuschließen.
4. Wenn Sie auf Vergleichen klicken, werden die konfigurierten Einstellungen in Spalten angezeigt.
5. Zum Anzeigen aller Einstellungen wählen Sie Alle Einstellungen anzeigen. Sie kehren zur Standardansicht zurück, indem Sie


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gemeinsame Einstellungen anzeigen auswählen.

## Festlegen der Richtlinienpriorität

Durch Festlegen der Richtlinienpriorität definieren Sie, welche Richtlinie Vorrang hat, wenn es Konflikte gibt. Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet.

Sie weisen Richtlinien Prioritäten zu, indem Sie ihnen unterschiedliche Prioritätswerte in Studio geben. Neue Richtlinien erhalten standardmäßig die niedrigste Priorität. Falls widersprüchliche Richtlinieneinstellungen auftreten, setzt eine Richtlinie mit einem höheren Prioritätswert (eine Priorität von "1" hat die höchste Priorität) eine Richtlinie mit einem niedrigeren Prioritätswert außer Kraft. Einstellungen werden nach der Priorität und dem Zustand der Einstellung, z. B. ob die Einstellung deaktiviert oder aktiviert ist, zusammengeführt. Jede deaktivierte Einstellung hat Vorrang vor einer aktivierten Einstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus. Wählen Sie die Registerkarte "Richtlinien" aus.
2. Wählen Sie eine Richtlinie.
3. Wählen Sie im Aktionsbereich Geringere Priorität oder Höhere Priorität.

## Ausnahmen

Wenn Sie Richtlinien für Benutzergruppen, Benutzergeräte oder Maschinen erstellen, werden Sie möglicherweise feststellen, dass für einige Mitglieder einer Gruppe Ausnahmen zu einigen Einstellungen erstellt werden müssen. Sie können Ausnahmen wie folgt erstellen:

- Erstellen Sie eine Richtlinie für die Gruppenmitglieder, für die Ausnahmen erforderlich sind, und stufen Sie die Richtlinie mit höherer Priorität ein als die Richtlinie für die gesamte Gruppe.
- Verwenden Sie den Modus Verweigern in einer Zuweisung, die Sie der Richtlinie hinzufügen.

Die Zuweisung im Modus Verweigern wendet eine Richtlinie nur auf Verbindungen an, die nicht den Zuweisungskriterien entsprechen. Beispielsweise könnte eine Richtlinie folgende Zuweisungen enthalten:

- Zuweisung A ist eine Client-IP-Adressenzuweisung, die den Bereich 208.77.88.* festlegt, und der Modus ist Zulassen
- Zuweisung B ist eine Benutzerzuweisung, die ein spezifisches Benutzerkonto angibt, und der Modus ist Verweigern

Die Richtlinie wird auf alle Benutzer angewendet, die sich mit IP-Adressen aus dem in Zuweisung A festgelegten Bereich bei der Site anmelden. Die Richtlinie wird aber nicht auf den Benutzer angewendet, der sich mit dem in Zuweisung B festgelegten Konto anmeldet, obwohl dem Computer dieses Benutzers eine IP-Adresse aus dem in Zuweisung A festgelegten Bereich zugewiesen wurde.

## Ermitteln der auf eine Verbindung angewendeten Richtlinien

Manchmal reagiert eine Verbindung nicht wie erwartet, weil mehrere Richtlinien gelten. Wenn eine Richtlinie mit einer höheren Priorität auf eine Verbindung angewendet wird, kann sie Einstellungen, die Sie in der ursprünglichen Richtlinie konfigurieren, außer Kraft setzen. Sie können ermitteln, wie die Richtlinieneinstellungen am Ende für eine Verbindung zusammengeführt werden, indem sie den Richtlinienergebnissatz berechnen.

Sie berechnen den Richtlinienergebnissatz mit folgenden Methoden:

- Verwenden Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung, um ein Verbindungsszenario zu simulieren und festzustellen, wie Citrix Richtlinien angewendet werden können. Sie können Bedingungen für ein Verbindungsszenario angeben, z. B. Domänencontroller, Benutzer, Citrix Richtlinienzuweisungsbeweiswerte und simulierte Umgebungseinstellungen wie langsame Netzwerkverbindungen. Der von dem Assistenten erstellte Bericht listet die Citrix


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Richtlinien auf, die in dem Szenario wahrscheinlich wirksam werden. Wenn Sie beim Controller als Domänenbenutzer angemeldet sind, berechnet der Assistent den Richtlinienergebnissatz anhand von Richtlinieneinstellungen für die Site und Active Directory-Gruppenrichtlinienobjekten.
- Verwenden Sie das Tool "Gruppenrichtlinienergebnisse", um einen Bericht zu erstellen, der beschreibt, welche Citrix Richtlinien für einen bestimmten Benutzer oder einen bestimmten Controller angewendet werden. Das Tool "Gruppenrichtlinienergebnisse" unterstützt Sie dabei, den aktuellen Zustand von Gruppenrichtlinienobjekten in der Umgebung zu evaluieren, und generiert einen Bericht, in dem beschrieben wird, wie diese Objekte, einschließlich Citrix Richtlinien, derzeit auf einen bestimmten Benutzer und Controller angewendet werden.

Sie können den Assistenten für die Citrix Gruppenrichtlinienmodellierung im Bereich "Aktionen" in Studio starten. Sie können beide Tools in der Gruppenrichtlinien-Verwaltungskonsole von Windows starten.

Wenn Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung oder das Tool "Gruppenrichtlinienergebnisse" über die Gruppenrichtlinien-Verwaltungskonsole ausführen, werden die mit Studio erstellten Site-Richtlinieneinstellungen nicht in den Richtlinienergebnissatz einbezogen.

Um sicherzustellen, dass Sie den umfassendsten Richtlinienergebnissatz erhalten, empfiehlt Citrix das Starten des Assistenten für die Citrix Gruppenrichtlinienmodellierung über Studio, es sei denn, Sie erstellen Richtlinien nur über die Gruppenrichtlinien-Verwaltungskonsole.

### Verwenden des Assistenten für die Citrix Gruppenrichtlinienmodellierung

Öffnen Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung mit einer der folgenden Optionen:
- Wählen Sie Richtlinien im Navigationsbereich von Studio, wählen Sie dann die Registerkarte "Modellierung" und dann im Aktionsbereich die Option Modellierungsassistenten starten.
- Starten Sie die Gruppenrichtlinien-Verwaltungskonsole (gpmc.msc), klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf Citrix Gruppenrichtlinienmodellierung und wählen Sie dann Citrix Gruppenrichtlinienmodellierungsassistent aus.

Folgen Sie den Anweisungen des Assistenten, um den Domänencontroller, Benutzer, Computer, Umgebungseinstellungen und Citrix Zuweisungskriterien für die Simulation auszuwählen. Wenn Sie auf Fertig stellen klicken, erstellt der Assistent einen Bericht mit den Modellierungsergebnissen. In Studio wird der Bericht im mittleren Bereich unter der Registerkarte Modellierung angezeigt.

Zum Anzeigen des Berichts wählen Sie Modellierungsbericht anzeigen.

### Problembehandlung bei Richtlinien

Für Benutzer, IP-Adressen und andere zugewiesene Objekte können mehrere Richtlinien gleichzeitig gelten. Dies kann zu Konflikten führen, wenn eine Richtlinie sich nicht wie erwartet verhält. Wenn Sie den Citrix Gruppenrichtlinienmodellierungsassistenten oder das Gruppenrichtlinienergebnisse-Tool ausführen, entdecken Sie möglicherweise, dass keine Richtlinien auf die Benutzerverbindungen angewendet werden. In diesen Fall sind Benutzer nicht von Richtlinieneinstellungen betroffen, wenn sie sich unter Bedingungen mit Anwendungen verbinden, die den Richtlinienkriterien entsprechen. Dies passiert in folgenden Fällen:
- Keine Richtlinie hat eine Zuweisung, die den Richtlinienkriterien entspricht.
- Richtlinien, die der Zuweisung entsprechen, haben keine konfigurierten Einstellungen.
- Richtlinien, die der Zuweisung entsprechen, sind deaktiviert.

Wenn Sie Richtlinieneinstellungen auf Verbindungen anwenden möchten, die bestimmten Kriterien entsprechen, stellen Sie Folgendes sicher:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Die Richtlinien, die auf diese Verbindungen angewendet werden sollen, sind aktiviert.
- In den Richtlinien, die Sie anwenden möchten, sind die geeigneten Einstellungen konfiguriert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Standardrichtlinieneinstellungen

Aug 17, 2016

Die folgenden Tabellen enthalten Richtlinieneinstellungen, die Standardeinstellungen und die VDA-Versionen, für die sie gelten.

## ICA

| Name | Standardeinstellung | VDA |
|---|---|---|
| Clientzwischenablagenumleitung | Zugelassen | Alle VDA-Versionen |
| Desktop starten | Nicht zugelassen | VDA für Server-OS 7 bis aktuelle Version |
| ICA-Listener - Verbindungstimeout | 120.000 Millisekunden | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| ICA-Listenerportnummer | 1494 | Alle VDA-Versionen |
| Starten nicht-veröffentlichter Programme bei Clientverbindung | Nicht zugelassen | VDA für Server-OS 7 bis aktuelle Version |
| Zum Schreiben in Clientzwischenablage zugelassene Formate | Keine Formate angegeben | VDA 7.6 bis aktuelle Version |
| Schreiben in Clientzwischenablage einschränken | Nicht zugelassen | VDA 7.6 bis aktuelle Version |
| Schreiben in Sitzungszwischenablage einschränken | Nicht zugelassen | VDA 7.6 bis aktuelle Version |
| Zum Schreiben in Sitzungszwischenablage zugelassene Formate | Keine Formate angegeben | VDA 7.6 bis aktuelle Version |

## ICA/Adobe Flash-Bereitstellung/Flash-Umleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Verhindern von Flash-Videofallback | Nicht konfiguriert | VDA 7.6 FP3 bis aktuelle Version |
| Fehler beim Verhindern von Flash-Videofallback *.swf | | VDA 7.6 FP3 bis aktuelle Version |

## ICA/Audio

| Name | Standardeinstellung | VDA |
|---|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Audio Plug & Play | Zugelassen | VDA für Server-OS 7 bis aktuelle Version |
| Audioqualität | Hoch - High Definition Audio | Alle VDA-Versionen |
| Clientaudioumleitung | Zugelassen | Alle VDA-Versionen |
| Clientmikrofonumleitung | Zugelassen | Alle VDA-Versionen |

ICA/Automatische Wiederverbindung von Clients

| Name | Standardeinstellung | VDA |
|---|---|---|
| Automatische Wiederverbindung von Clients | Zugelassen | Alle VDA-Versionen |
| Authentifizierung bei automatischer Wiederverbindung von Clients | Keine Authentifizierung erforderlich | Alle VDA-Versionen |
| Protokollierung der automatischen Wiederverbindung von Clients | Kein Protokollieren von Wiederverbindungsereignissen | Alle VDA-Versionen |

ICA/Bandwidth

| Name | Standardeinstellung | VDA |
|---|---|---|
| Bandbreitenlimit für die Audioumleitung | 0 KBit/s | Alle VDA-Versionen |
| Bandbreitenlimit für die Audioumleitung (Prozent) | 0 | Alle VDA-Versionen |
| Bandbreitenlimit für Client-USB-Geräteumleitung | 0 KBit/s | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) | 0 | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bandbreitenlimit für Zwischenablagenumleitung | 0 KBit/s | Alle VDA-Versionen |
| Bandbreitenlimit für Zwischenablagenumleitung (Prozent) | 0 | Alle VDA-Versionen |
| Bandbreitenlimit für COM-Portumleitung | 0 KBit/s | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Bandbreitenlimit für COM-Portumleitung (Prozent) | 0 | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Bandbreitenlimit für Dateiumleitung | 0 KBit/s | Alle VDA-Versionen |
| | | |
| Bandbreitenlimit für Dateiumleitung (Prozent) | 0 | Alle VDA-Versionen |
| Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung | 0 KBit/s | VDA 5.5, 5.6 FP 1, VDA für Server-OS 7 und VDA für Desktop-OS 7 bis zum aktuellen VDA für Server-OS und VDA für Desktop-OS |
| Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent) | 0 | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bandbreitenlimit für LPT-Portumleitung | 0 KBit/s | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Bandbreitenlimit für LPT-Portumleitung (Prozent) | 0 | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Bandbreitenlimit für Sitzung insgesamt | 0 KBit/s | Alle VDA-Versionen |
| Bandbreitenlimit für Druckerumleitung | 0 KBit/s | Alle VDA-Versionen |
| Bandbreitenlimit für Druckerumleitung (Prozent) | 0 | Alle VDA-Versionen |
| Bandbreitenlimit für TWAIN-Geräteumleitung | 0 KBit/s | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) | 0 | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Clientsensoren

| Name | Standardeinstellung | VDA |
|---|---|---|
| Anwendungen können den physischen Standort des Clientgeräts verwenden | Nicht zugelassen | VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Desktopbenutzeroberfläche

| Name | Standardeinstellung | VDA |
|---|---|---|
| Desktopgestaltungsumleitung | Deaktiviert (7.6 FP3 bis aktuelle Version) | VDA 5.6, VDA für Desktopbetriebssysteme 7 bis aktuelle VDA-Version |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| | Aktiviert (5.6 bis 7.6 FP2) | |
| Grafikqualität Desktopgestaltung | Mittel | VDA 5.6, VDA für Desktopbetriebssysteme 7 bis aktuelle Version |
| Desktophintergrund | Zugelassen | Alle VDA-Versionen |
| Menüanimation | Zugelassen | Alle VDA-Versionen |
| Fensterinhalt beim Verschieben anzeigen | Zugelassen | Alle VDA-Versionen |

ICA/Endbenutzerüberwachung

| Name | Standardeinstellung | VDA |
|---|---|---|
| ICA-Roundtripberechnung | Aktiviert | Alle VDA-Versionen |
| Intervall für ICA-Roundtripberechnung | 15 Sekunden | Alle VDA-Versionen |
| ICA-Roundtrip für Verbindungen im Leerlauf berechnen | Deaktiviert | Alle VDA-Versionen |

ICA/Enhanced Desktop Experience

| Name | Standardeinstellung | VDA |
|---|---|---|
| Enhanced Desktop Experience | Zugelassen | VDA für Server-OS 7 bis aktuelle Version |

ICA/Dateiumleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Clientlaufwerke automatisch verbinden | Zugelassen | Alle VDA-Versionen |
| Clientlaufwerkumleitung | Zugelassen | Alle VDA-Versionen |
| Lokale Clientfestplattenlaufwerke | Zugelassen | Alle VDA-Versionen |
| Clientdiskettenlaufwerke | Zugelassen | Alle VDA-Versionen |
| Clientnetzlaufwerke | Zugelassen | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Optische Clientlaufwerke | Zugelassen | Alle VDA-Versionen |
| Clientwechsellaufwerke | Zugelassen | Alle VDA-Versionen |
| Host-zu-Client-Umleitung | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version |
| Clientlaufwerksbuchstaben erhalten | Deaktiviert | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Schreibgeschützter Zugriff auf Clientlaufwerke | Deaktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Umleitung spezieller Ordner | Zugelassen | Nur Webinterface-Bereitstellungen; VDA für Server-OS 7 bis aktuelle Version |
| Asynchrones Schreiben verwenden | Deaktiviert | Alle VDA-Versionen |

ICA/Graphics

| Name | Standardeinstellung | VDA |
|---|---|---|
| Visuell verlustfreie Komprimierung zulassen | Deaktiviert | VDA 7.6 bis aktuelle Version |
| Anzeigespeicherlimit | 65536 KBit | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Herabsetzungspräferenz für Anzeigemodus | Zuerst Farbtiefe herabsetzen | Alle VDA-Versionen |
| Dynamische Fenstervorschau | Aktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bildzwischenspeicherung | Aktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Legacygrafikmodus | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Maximal zugelassene Farbtiefe | 32 Bit pro Pixel | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | | |
|---|---|---|
| Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version |
| Warteschlange und Verwerfen | Aktiviert | Alle VDA-Versionen |
| Verwenden von Videocodec für die Komprimierung | Videocodec verwenden, wenn bevorzugt | VDA 7.6 FP3 bis aktuelle Version |

ICA/Graphics/Caching

| Name | Standardeinstellung | VDA |
|---|---|---|
| Schwellenwert für permanenten Cache | 3000000 Bit/s | VDA für Server-OS 7 bis aktuelle Version |

ICA/Graphics/Framehawk

| Name | Standardeinstellung | VDA |
|---|---|---|
| Framehawk-Anzeigekanal | Deaktiviert | VDA 7.6 FP2 bis aktuelle Version |
| Portbereich für Framehawk-Anzeigekanal | 3224,3324 | VDA 7.6 FP2 bis aktuelle Version |

ICA/Keep-Alive

| Name | Standardeinstellung | VDA |
|---|---|---|
| ICA-Keep-Alive - Timeout | 60 Sekunden | Alle VDA-Versionen |
| ICA-Keep-Alives | Keine ICA-Keep-Alive-Meldungen senden | Alle VDA-Versionen |

ICA/Zugriff auf lokale Anwendungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Lokalen App-Zugriff zulassen | Nicht zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| URL-Umleitungssperrliste | Keine Sites angegeben | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| URL-Umleitungspositivliste | Keine Sites angegeben | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICA/Mobilerfahrung

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Automatische Anzeige der Tastatur | Nicht zugelassen | VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Für Fingereingabe optimierten Desktop starten | Zugelassen | VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version<br><br>Diese Einstellung ist deaktiviert und für Windows 10-Maschinen nicht verfügbar. |
| Kombinationsfelder remoten | Nicht zugelassen | VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Multimedia

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Videoqualität beschränken | Nicht konfiguriert | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Multimediakonferenzen | Zugelassen | Alle VDA-Versionen |
| Optimierung von Windows Media-Multimediaumleitung über WAN | Zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden | Nicht zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Richtlinieneinstellung für Videolastverwaltung | Nicht konfiguriert | VDA 7.6 FP3 bis aktuelle Version |
| Clientseitiger Abruf von Windows Media-Inhalten | Zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | | |
|---|---|---|
| Windows Media-Umleitung | Zugelassen | Alle VDA-Versionen |
| Windows Media-Umleitungspuffergröße | 5 Sekunden | VDA 5, 5.5, 5.6 FP1 |
| Verwendung von Windows Media-Umleitungspuffergröße | Deaktiviert | VDA 5, 5.5, 5.6 FP1 |

ICA/Multistreamverbindungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Audio über UDP | Zugelassen | VDA für Server-OS 7 bis aktuelle Version |
| Audio-UDP-Portbereich | 16500, 16509 | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Multiportrichtlinie | Primärer Port (2598) hat hohe Priorität | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Multistreamcomputereinstellung | Deaktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Multistreambenutzereinstellung | Deaktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA\Portumleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Client-COM-Ports automatisch verbinden | Deaktiviert | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Client-LPT-Ports automatisch verbinden | Deaktiviert | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Client-COM-Portumleitung | Nicht zugelassen | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |
| Client-LPT-Portumleitung | Nicht zugelassen | Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren. |

ICA/Printing

| Name | Standardeinstellung | VDA |
|---|---|---|
| Clientdruckerumleitung | Zugelassen | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Standarddrucker | Hauptdrucker des Clients als Standarddrucker verwenden | Alle VDA-Versionen |
| Druckerzuweisungen | Der aktuelle Drucker des Benutzers wird als Standarddrucker in der Sitzung verwendet. | Alle VDA-Versionen |
| Ereignisprotokollpräferenz für die automatische Druckererstellung | Fehler und Warnungen protokollieren | Alle VDA-Versionen |
| Sitzungsdrucker | Keine Drucker angegeben | Alle VDA-Versionen |
| Warten bis Drucker erstellt sind (Desktop) | Deaktiviert | Alle VDA-Versionen |

ICA/Drucken/Clientdrucker

| Name | Standardeinstellung | VDA |
|---|---|---|
| Clientdrucker automatisch erstellen | Alle Clientdrucker automatisch erstellen | Alle VDA-Versionen |
| Generischen universellen Drucker automatisch erstellen | Deaktiviert | Alle VDA-Versionen |
| Clientdruckernamen | Standarddruckernamen | Alle VDA-Versionen |
| Direkte Verbindungen zu Druckservern | Aktiviert | Alle VDA-Versionen |
| Druckertreiberzuordnung und -kompatibilität | Keine Regeln angegeben | Alle VDA-Versionen |
| Speicherung von Druckereigenschaften | Im Profil speichern, wenn sie nicht auf dem Client gespeichert sind | Alle VDA-Versionen |
| Gespeicherte und wiederhergestellte Clientdrucker | Zugelassen | VDA 5, 5.5, 5.6 FP1 |

ICA/Printing/Drivers

| Name | Standardeinstellung | VDA |
|---|---|---|
| Automatische Installation von mitgelieferten Druckertreibern | Aktiviert | Alle VDA-Versionen |
| Priorität universeller Treiber | EMF, XPS, PCL5c, PCL4, PS | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Verwendung universeller Druckertreiber | Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist | Alle VDA-Versionen |

ICA/Drucken/Universeller Druckserver

| Name | Standardeinstellung | VDA |
|---|---|---|
| Universellen Druckserver aktivieren | Deaktiviert | Alle VDA-Versionen |
| Port für Druckdatenstrom des universellen Druckservers (CGP) | 7229 | Alle VDA-Versionen |
| Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s) | 0 | Alle VDA-Versionen |
| Port für universellen Druckserverwebdienst (HTTP/SOAP) | 8080 | Alle VDA-Versionen |
| Universelle Druckserver für den Lastausgleich | | VDA 7.9 bis aktuelle Version |
| Außer-Betrieb-Schwellenwert für universelle Druckserver | 180 (Sekunden) | VDA 7.9 bis aktuelle Version |

ICA/Drucken/Universelles Drucken

| Name | Standardeinstellung | VDA |
|---|---|---|
| Universelles Drucken - EMF-Verarbeitungsmodus | Direkt zum Drucker spoolen | Alle VDA-Versionen |
| Universelles Drucken - Bildkomprimierungslimit | Beste Qualität (verlustfreie Komprimierung) | Alle VDA-Versionen |
| Universelles Drucken - Optimierungsstandards | Bildkomprimierung<br>• Gewünschte Bildqualität=Standardqualität<br>• Heavyweight-Komprimierung aktivieren=False<br><br>Zwischenspeichern von Bildern und Schriftarten<br>• Zwischenspeichern eingebetteter Bilder zulassen=True | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| | • Zwischenspeichern eingebetteter Schriftarten zulassen=True<br>Nicht-Administratoren können diese Einstellungen anpassen=False | |
| Universelles Drucken - Vorschaueinstellung | Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden | Alle VDA-Versionen |
| Universelles Drucken - Druckqualitätslimit | Kein Limit | Alle VDA-Versionen |

ICA/Security

| Name | Standardeinstellung | VDA |
|---|---|---|
| SecureICA-Mindestverschlüsselungsgrad | Standard | VDA für Server-OS 7 bis aktuelle Version |

ICA/Serverlimits

| Name | Standardeinstellung | VDA |
|---|---|---|
| Serverleerlauf-Zeitintervall | 0 Millisekunden | VDA für Server-OS 7 bis aktuelle Version |

ICA/Sitzungslimits

| Name | Standardeinstellung | VDA |
|---|---|---|
| Timer für getrennte Sitzung | Deaktiviert | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Getrennte Sitzungen - Timerintervall | 1440 Minuten | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Sitzungsverbindungstimer | Deaktiviert | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Sitzungsverbindung - Timerintervall | 1440 Minuten | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Sitzungsleerlauftimer | Enabledf | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |
| Sitzungsleerlauf - Timerintervall | 1440 Minuten | VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Sitzungszuverlässigkeit


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Sitzungszuverlässigkeit - Verbindungen | Zugelassen | Alle VDA-Versionen |
| Sitzungszuverlässigkeit - Portnummer | 2598 | Alle VDA-Versionen |
| Sitzungszuverlässigkeit - Timeout | 180 Sekunden | Alle VDA-Versionen |

ICA/Zeitzonensteuerung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Lokale Zeitzone für Legacyclients schätzen | Aktiviert | VDA für Server-OS 7 bis aktuelle Version |
| Lokale Zeit des Clients verwenden | Serverzeitzone verwenden | Alle VDA-Versionen |

ICA/TWAIN-Geräte

| Name | Standardeinstellung | VDA |
|---|---|---|
| TWAIN-Geräteumleitung für Client | Zugelassen | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| TWAIN-Komprimierungsgrad | Mittel | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/USB-Geräte

| Name | Standardeinstellung | VDA |
|---|---|---|
| Regeln für die Client-USB-Geräteoptimierung | Keine Regeln angegeben | VDA 7.6 FP3 bis aktuelle Version |
| Client-USB-Geräteumleitung | Nicht zugelassen | Alle VDA-Versionen |
| Regeln für die Client-USB-Geräteumleitung | Keine Regeln angegeben | Alle VDA-Versionen |
| Client-USB-Geräteumleitung für Plug & Play-Geräte | Zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Visuelle Anzeige


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Bevorzugte Farbtiefe für einfache Grafiken | 24 Bit pro Pixel | VDA 7.6 FP3 bis aktuelle Version |
| Frameratesollwert | 30 F/s | Alle VDA-Versionen |
| Bildqualität | Mittel | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Visuelle Anzeige/Bewegtbilder

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Mindestbildqualität | Normal | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Bewegtbildkomprimierung | Aktiviert | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Grad der progressiven Komprimierung | Keine | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Schwellenwert für progressive Komprimierung | 2147483647 KBit/s | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Mindestframeratesollwert | 10 F/s | VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

ICA/Visuelle Anzeige/Festbilder

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Zusätzliche Farbkomprimierung | Deaktiviert | Alle VDA-Versionen |
| Schwellenwert für zusätzliche Farbkomprimierung | 8192 KBit/s | Alle VDA-Versionen |
| Heavyweight-Komprimierung | Deaktiviert | Alle VDA-Versionen |
| Grad der verlustreichen Komprimierung | Mittel | Alle VDA-Versionen |
| Schwellenwert für verlustreiche Komprimierung | 2147483647 KBit/s | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICA/WebSockets

| Name | Standardeinstellung | VDA |
|---|---|---|
| WebSockets-Verbindungen | Nicht zugelassen | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| WebSockets-Portnummer | 8008 | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Vertrauenswürdige WebSockets-Ursprungsserverliste | Bei Verwendung des Platzhalters * wird allen Receiver für Web-URLs vertraut. | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

Load Management

| Name | Standardeinstellung | VDA |
|---|---|---|
| Toleranzwert für gleichzeitige Anmeldungen | 2 | VDA für Server-OS 7 bis aktuelle Version |
| CPU-Nutzung | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version |
| CPU-Nutzung ausschließlich Prozesspriorität | Unter normal oder niedrig | VDA für Server-OS 7 bis aktuelle Version |
| Datenträgernutzung | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version |
| Sitzungshöchstanzahl | 250 | VDA für Server-OS 7 bis aktuelle Version |
| Speichernutzung | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version |
| Speichernutzung - Ausgangslast | Nulllast: 768 MB | VDA für Server-OS 7 bis aktuelle Version |

Profilverwaltung/Erweiterte Einstellungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Automatische Konfiguration deaktivieren | Deaktiviert | Alle VDA-Versionen |
| Benutzer bei Problem abmelden | Deaktiviert | Alle VDA-Versionen |
| Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien | 5 | Alle VDA-Versionen |
| Internet-Cookiedateien bei Abmeldung verarbeiten | Deaktiviert | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|

Profilverwaltung/Grundeinstellungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Aktiv zurückschreiben | Deaktiviert | Alle VDA-Versionen |
| Profilverwaltung aktivieren | Deaktiviert | Alle VDA-Versionen |
| Ausgeschlossene Gruppen | Deaktiviert: Mitglieder aller Benutzergruppen werden verarbeitet. | Alle VDA-Versionen |
| Unterstützung von Offlineprofilen | Deaktiviert | Alle VDA-Versionen |
| Pfad zum Benutzerspeicher | Windows | Alle VDA-Versionen |
| Anmeldungen lokaler Administratoren verarbeiten | Deaktiviert | Alle VDA-Versionen |
| Verarbeitete Gruppen | Deaktiviert: Mitglieder aller Benutzergruppen werden verarbeitet. | Alle VDA-Versionen |

Profilverwaltung/Plattformübergreifende Einstellungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Benutzergruppen für plattformübergreifende Einstellungen | Deaktiviert: Alle in Verarbeitete Gruppen angegebenen Benutzergruppen werden verarbeitet | Alle VDA-Versionen |
| Plattformübergreifende Einstellungen aktivieren | Deaktiviert | Alle VDA-Versionen |
| Pfad zu plattformübergreifenden Definitionen | Deaktiviert: Kein Pfad angegeben. | Alle VDA-Versionen |
| Pfad zum Speicher für plattformübergreifende Einstellungen | Deaktiviert: Windows\PM_CM wird verwendet. | Alle VDA-Versionen |
| Quelle für plattformübergreifende Einstellungen | Deaktiviert | Alle VDA-Versionen |

Profilverwaltung/Dateisystem/Ausschlüsse

| Name | Standardeinstellung | VDA |
|---|---|---|
| Ausschlussliste - Verzeichnisse | Deaktiviert: Alle Ordner im Benutzerprofil werden synchronisiert. | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Ausschlussliste - Dateien | Deaktiviert: Alle Dateien im Benutzerprofil werden synchronisiert. | Alle VDA-Versionen |

Profilverwaltung/Dateisystem/Synchronisierung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Zu synchronisierende Verzeichnisse | Deaktiviert: Nur nicht ausgeschlossene Ordner werden synchronisiert. | Alle VDA-Versionen |
| Zu synchronisierende Dateien | Deaktiviert: Nur nicht ausgeschlossene Dateien werden synchronisiert. | Alle VDA-Versionen |
| Zu spiegelnde Ordner | Deaktiviert: Es werden keine Ordner gespiegelt. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Administratorzugriff gewähren | Deaktiviert | Alle VDA-Versionen |
| Domänennamen einschließen | Deaktiviert | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/AppData(Roaming)

| Name | Standardeinstellung | VDA |
|---|---|---|
| AppData(Roaming)-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für AppData(Roaming) | Inhalte werden zu dem in der Richtlinieneinstellung AppData(Roaming)-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Kontakte

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Kontakte'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Kontakte' | Inhalte werden zu dem in der Richtlinieneinstellung 'Kontakte'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Desktop


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Desktop'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Desktop' | Inhalte werden zu dem in der Richtlinieneinstellung 'Desktop'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Dokumente

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Dokumente'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Dokumente' | Inhalte werden zu dem in der Richtlinieneinstellung 'Dokumente'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Downloads

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Downloads'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Downloads' | Inhalte werden zu dem in der Richtlinieneinstellung 'Downloads'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Favoriten

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Favoriten'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Favoriten' | Inhalte werden zu dem in der Richtlinieneinstellung 'Favoriten'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Links

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Links'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Links' | Inhalte werden zu dem in der Richtlinieneinstellung 'Links'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Profilverwaltung/Ordnerumleitung/Musik

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Musik'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Musik' | Inhalte werden zu dem in der Richtlinieneinstellung 'Musik'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Bilder

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Bilder'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Bilder' | Inhalte werden zu dem in der Richtlinieneinstellung 'Bilder'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Gespeicherte Spiele

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Gespeicherte Spiele'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Gespeicherte Spiele' | Inhalte werden zu dem in der Richtlinieneinstellung 'Gespeicherte Spiele'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Suchen

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Suchen'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Suchen' | Inhalte werden zu dem in der Richtlinieneinstellung 'Suchen'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Ordnerumleitung/Startmenü

| Name | Standardeinstellung | VDA |
|---|---|---|
| Startmenü-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Startmenü' | Inhalte werden zu dem in der Richtlinieneinstellung 'Startmenü'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|

Profilverwaltung/Ordnerumleitung/Videos

| Name | Standardeinstellung | VDA |
|---|---|---|
| 'Videos'-Pfad | Deaktiviert: Kein Speicherort angegeben. | Alle VDA-Versionen |
| Umleitungseinstellungen für 'Videos' | Inhalte werden zu dem in der Richtlinieneinstellung 'Videos'-Pfad angegebenen UNC-Pfad umgeleitet. | Alle VDA-Versionen |

Profilverwaltung/Protokolleinstellungen

| Name | Standardeinstellung | VDA |
|---|---|---|
| Active Directory-Aktionen | Deaktiviert | Alle VDA-Versionen |
| Allgemeine Informationen | Deaktiviert | Alle VDA-Versionen |
| Allgemeine Warnungen | Deaktiviert | Alle VDA-Versionen |
| Protokollierung aktivieren | Deaktiviert | Alle VDA-Versionen |
| Dateisystemaktionen | Deaktiviert | Alle VDA-Versionen |
| Dateisystembenachrichtigungen | Deaktiviert | Alle VDA-Versionen |
| Abmeldung | Deaktiviert | Alle VDA-Versionen |
| Anmeldebildschirm | Deaktiviert | Alle VDA-Versionen |
| Max. Größe der Protokolldatei | 1048576 | Alle VDA-Versionen |
| Pfad zur Protokolldatei | Deaktiviert: Protokolldateien werden im Standardspeicherort gespeichert: %SystemRoot%\System32\Logfiles\UserProfileManager. | Alle VDA-Versionen |
| Persönliche Benutzerinformationen | Deaktiviert | Alle VDA-Versionen |
| Richtlinienwerte bei Anmeldung und Abmeldung | Deaktiviert | Alle VDA-Versionen |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Registrierungsaktionen | Deaktiviert | Alle VDA-Versionen |
| Registrierungsunterschiede bei der Abmeldung | Deaktiviert | Alle VDA-Versionen |

Profilverwaltung/Profilverarbeitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Verzögerung vor dem Löschen von zwischengespeicherten Profilen | 0 | Alle VDA-Versionen |
| Lokal zwischengespeicherte Profile nach Abmeldung löschen | Deaktiviert | Alle VDA-Versionen |
| Behandlung von Konflikten lokaler Profile | Lokales Profil verwenden | Alle VDA-Versionen |
| Migration vorhandener Profile | Lokal und Roaming | Alle VDA-Versionen |
| Pfad zum Vorlagenprofil | Deaktiviert: Neue Benutzerprofile werden von dem Standardbenutzerprofil auf dem Gerät erstellt, auf dem sich ein Benutzer als Erstes anmeldet. | Alle VDA-Versionen |
| Vorlagenprofil überschreibt lokales Profil | Deaktiviert | Alle VDA-Versionen |
| Vorlagenprofil überschreibt Roamingprofil | Deaktiviert | Alle VDA-Versionen |
| Als verbindliches Citrix Profil für alle Anmeldungen verwendete Vorlagenprofil | Deaktiviert | Alle VDA-Versionen |

Profilverwaltung/Registrierung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Ausschlussliste | Deaktiviert: Alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet, wenn ein Benutzer sich abmeldet. | Alle VDA-Versionen |
| Aufnahmeliste | Deaktiviert: Alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet, wenn ein Benutzer sich abmeldet. | Alle VDA-Versionen |

Profilverwaltung/Gestreamte Benutzerprofile

| Name | Standardeinstellung | VDA |
|---|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Immer zwischenspeichern | Deaktiviert | Alle VDA-Versionen |
| Immer Cachegröße | 0 MBit | Alle VDA-Versionen |
| Profilstreaming | Deaktiviert | Alle VDA-Versionen |
| Gruppen mit gestreamten Benutzerprofilen | Deaktiviert: Alle Benutzerprofile in einer Organisationseinheit werden normal verarbeitet. | Alle VDA-Versionen |
| Timeout für bevorstehende Sperrdateien (Tage) | 1 Tag | Alle VDA-Versionen |

Receiver

| Name | Standardeinstellung | VDA |
|---|---|---|
| StoreFront-Kontenliste | Keine Stores angegeben | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |

Virtual Delivery Agent

| Name | Standardeinstellung | VDA |
|---|---|---|
| IPv6-Netzwerkmaske für Controllerregistrierung | Keine Netzwerkmaske angegeben. | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Controllerregistrierungsport | 80 | Alle VDA-Versionen |
| Controller-SIDs | Keine SIDs angegeben | Alle VDA-Versionen |
| Controller | Keine Controller angegeben | Alle VDA-Versionen |
| Automatische Controllerupdates aktivieren | Aktiviert | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Nur IPv6-Controllerregistrierung verwenden | Deaktiviert | VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version |
| Site-GUID | Kein GUID angegeben. | Alle VDA-Versionen |

Virtuelle IP

| Name | Standardeinstellung | VDA |
|---|---|---|


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Name | Standardeinstellung | VDA |
|---|---|---|
| Virtuelle IP - Loopbackunterstützung | Deaktiviert | VDA 7.6 bis aktuelle Version |
| Virtuelle IP - Programme für virtuelles Loopback | Keine | VDA 7.6 bis aktuelle Version |

HDX 3D Pro

| Name | Standardeinstellung | VDA |
|---|---|---|
| Verlustfrei aktivieren | Aktiviert | VDA 5.5, 5.6 FP1 |
| HDX3DPro-Qualitätseinstellungen | | VDA 5.5, 5.6 FP1 |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Referenz für Richtlinieneinstellungen

Jul 08, 2016

Richtlinien enthalten Einstellungen, die gelten, wenn die Richtlinie angewendet wird. Die Beschreibungen in diesem Abschnitt geben auch an, ob zusätzliche Einstellungen zum Aktivieren eines Features erforderlich sind oder ob Einstellungen sich ähnlich sind.

### Kurzanleitung

Die folgenden Tabellen listen die Einstellungen auf, die Sie in einer Richtlinie konfigurieren können. In der linken Spalte finden Sie die Aufgaben, in der rechten die dazugehörigen Einstellungen.

## Audio

| Aufgabe | Richtlinieneinstellung |
|---|---|
| Steuern der Verwendung mehrerer Audiogeräte | Audio Plug & Play |
| Steuern, ob Audioeingaben vom Mikrofon auf dem Benutzergerät zulässig sind | Clientmikrofonumleitung |
| Steuern der Audioqualität auf dem Benutzergerät | Audioqualität |
| Steuern der Audiozuordnung für Lautsprecher am Benutzergerät | Clientaudioumleitung |

## Bandbreite für Benutzergeräte

| Beschränken der Bandbreite | Richtlinieneinstellung |
|---|---|
| Clientaudiozuordnung | • Bandbreitenlimit für die Audioumleitung oder<br>• Bandbreitenlimit für die Audioumleitung (Prozent) |
| Kopieren und Einfügen mit der lokalen Zwischenablage | • Bandbreitenlimit für Zwischenablagenumleitung oder<br>• Bandbreitenlimit für Zwischenablagenumleitung (Prozent) |
| Zugriff auf lokale Clientlaufwerke in einer Sitzung | • Bandbreitenlimit für Dateiumleitung oder<br>• Bandbreitenlimit für Dateiumleitung (Prozent) |
| HDX MediaStream-Multimediabeschleunigung | • Bandbreitenlimit für HDX MediaStream- |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Beschränken der Bandbreite | Richtlinieneinstellung |
| --- | --- |
| | Multimediabeschleunigung oder<br>• Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent) |
| Clientsitzung | Bandbreitenlimit für Sitzung insgesamt |
| Drucken | • Bandbreitenlimit für Druckerumleitung oder<br>• Bandbreitenlimit für Druckerumleitung (Prozent) |
| TWAIN-Geräte (wie Kameras oder Scanner) | • Bandbreitenlimit für TWAIN-Geräteumleitung oder<br>• Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) |
| USB-Geräte | • Bandbreitenlimit für Client-USB-Geräteumleitung oder<br>• Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) |

## Umleitung von Clientlaufwerken und Benutzergeräten

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern, ob Laufwerke des Benutzergeräts verbunden werden, wenn Benutzer sich am Server anmelden | Clientlaufwerke automatisch verbinden |
| Steuern der Datenübertragung mit Kopier- und Einfügeoperationen zwischen dem Server und der lokalen Zwischenablage | Clientzwischenablagenumleitung |
| Steuern der Laufwerkzuordnung des Benutzergeräts | Clientlaufwerkumleitung |
| Steuern, ob die lokalen Festplatten des Benutzers in einer Sitzung verfügbar sind | • Lokale Clientlaufwerke und<br>• Clientlaufwerkumleitung |
| Steuern, ob die lokalen Diskettenlaufwerke des Benutzers in einer Sitzung verfügbar sind | • Clientdiskettenlaufwerke und<br>• Clientlaufwerkumleitung |
| Steuern, ob die Netzlaufwerke des Benutzers in einer Sitzung verfügbar sind | • Clientnetzlaufwerke und<br>• Clientlaufwerkumleitung |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern, ob die lokalen CD-, DVD- oder Blu-ray-Laufwerke des Benutzers in einer Sitzung verfügbar sind | • Optische Clientlaufwerke und<br>• Clientlaufwerkumleitung |
| Steuern, ob die lokalen Clientwechseldatenträger des Benutzers in einer Sitzung verfügbar sind | • Clientwechsellaufwerke und<br>• Clientlaufwerkumleitung |
| Steuern, ob TWAIN-Geräte, wie Scanner und Kameras, in einer Sitzung verfügbar sind und Steuern der Komprimierung bei der Übertragung von Bilddaten | • TWAIN-Geräteumleitung für Client<br>• TWAIN-Umleitung |
| Steuern, ob die USB-Geräte in einer Sitzung verfügbar sind | • Client-USB-Geräteumleitung und<br>• Regeln für die Client-USB-Geräteumleitung |
| Geschwindigkeit beim Schreiben und Kopieren von Dateien auf einen Clientdatenträger über ein WAN erhöhen | Asynchrones Schreiben verwenden |

## Inhaltsumleitung

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern der Verwendung der Inhaltsumleitung vom Server zum Benutzergerät | Host-zu-Client-Umleitung |

## Desktopbenutzeroberfläche

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern, ob der Desktophintergrund in Benutzersitzungen angezeigt wird | Desktophintergrund |
| Anzeigen des Fensterinhalts beim Verschieben des Fensters | Fensterinhalt beim Verschieben anzeigen |

## Grafiken & Multimedia

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern der maximalen Anzahl von Frames pro Sekunde, die an Benutzergeräte von virtuellen Desktops gesendet werden | Frameratesollwert |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern der visuellen Qualität der auf dem Benutzergerät angezeigten Bilder | Bildqualität |
| Steuern, ob Flash-Inhalte in Sitzungen wiedergegeben werden | Flash-Standardverhalten |
| Steuern, ob Flash-Inhalte auf Websites in Sitzungen angezeigt werden | • URL-Liste für serverseitigen Flash-Inhaltsabruf<br>• Flash-URL-Kompatibilitätsliste<br>• Einstellung der Richtlinie zum Verhindern von Videofallback<br>• Fehler beim Verhindern von Flash-Videofallback *.swf |

## Priorisieren des Multistream-Netzwerkdatenverkehrs

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Angeben der Ports für ICA-Datenübertragungen über mehrere Verbindungen und Festlegen der Netzwerkprioritäten | Multiportrichtlinie |
| Aktivieren der Unterstützung von Multistreamverbindungen zwischen Servern und Benutzergeräten | Multistream (Computer- und Benutzereinstellungen) |

## Drucken

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern der Clientdruckererstellung auf dem Benutzergerät | o Clientdrucker automatisch erstellen und<br>o Clientdruckerumleitung |
| Steuern des Speicherorts für die Druckereigenschaften | Speicherung von Druckereigenschaften |
| Steuern, ob Druckanfragen vom Client oder vom Server verarbeitet werden | Direkte Verbindungen zu Druckservern |
| Steuern, ob Benutzer auf Drucker zugreifen können, die an die Benutzergeräte angeschlossen sind | Clientdruckerumleitung |
| Steuern, ob bei der automatischen Erstellung von Client- und Netzwerkdruckern native Windows-Treiber installiert werden | Automatische Installation von mitgelieferten Druckertreibern |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Steuern, wann der universelle Druckertreiber verwendet wird | Verwendung universeller Druckertreiber |
| Wählen des Druckers anhand von Sitzungsinformationen eines mobilen Benutzers | Standarddrucker |
| Lastausgleich und Failover-Schwellenwert für universellen Druckserver festlegen | o Universelle Druckserver für den Lastausgleich<br>o Außer-Betrieb-Schwellenwert für universelle Druckserver |

Hinweis: Richtlinien können nicht zum Aktivieren eines Bildschirmschoners in einer Desktop- oder Anwendungssitzung verwendet werden. Wenn Benutzer einen Bildschirmschoner benötigen, muss dieser auf dem Benutzergerät eingerichtet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "ICA"

Jul 08, 2016

Der Abschnitt "ICA" enthält Richtlinieneinstellungen für ICA-Listenerverbindungen und die Zwischenablagenzuordnung.

## Clientzwischenablagenumleitung

Mit dieser Einstellung legen Sie fest, ob die Zwischenablage auf dem Clientgerät der Zwischenablage auf dem Server zugeordnet wird.

Standardmäßig ist die Umleitung der Zwischenablage zugelassen.

Wenn Sie verhindern möchten, dass Daten durch Kopieren und Einfügen über die Zwischenablage zwischen einer Sitzung und der lokalen Zwischenablage übertragen werden, wählen Sie Nicht zugelassen. Benutzer können weiterhin die Zwischenablage für das Kopieren von Daten zwischen Anwendungen einsetzen, die in Sitzungen ausgeführt werden.

Nachdem diese Einstellung zugelassen wurde, konfigurieren Sie die maximal zulässige Bandbreite, die die Zwischenablage in einer Clientverbindung verbrauchen darf. Verwenden Sie dazu die Einstellung Bandbreitenlimit für Zwischenablagenumleitung oder Bandbreitenlimit für Zwischenablagenumleitung (Prozent).

## Zum Schreiben in Clientzwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Clientzwischenablage einschränken aktiviert ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Mit dieser Einstellung können jedoch bestimmte Datenformate für die Zwischenablage des Clientendpunkts freigegeben werden. Um diese Einstellung zu verwenden, aktivieren Sie sie und fügen Sie die zulässigen Formate hinzu.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML-Format

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** zugelassen ist.
- Stellen Sie sicher, dass **Schreiben in Clientzwischenablage einschränken** aktiviert ist.
- Fügen Sie einen Eintrag für **HTML-Format** (und alle anderen Formate, die unterstützt werden sollen) unter **Zum Schreiben in Clientzwischenablage zugelassene Formate** hinzu.

**Hinweis:** Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (HTML-Format) werden alle vorhandenen Skripts von der Quelle des kopierten Inhalts an das Ziel kopiert. Vergewissern Sie sich vor dem Kopieren, dass eine Vertrauensstellung zur Quelle besteht. Wenn Sie Inhalte mit Skripts kopieren, werden diese nur aktiviert, wenn Sie die Zieldatei als HTML-Datei speichern und ausführen.

Zusätzliche benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung wird nicht angewendet, wenn Clientzwischenablagenumleitung oder Schreiben in Clientzwischenablage einschränken auf "Nicht zugelassen" festgelegt sind.

### Desktop starten

Mit dieser Einstellung legen Sie fest, ob Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zu einer Sitzung auf dem VDA herstellen können.

Standardmäßig können Benutzer ohne Administratorrechte keine Verbindung zu diesen Sitzungen herstellen.

Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind und eine RDP-Verbindung verwenden. Diese Benutzer können eine Verbindung zum VDA herstellen, unabhängig davon, ob diese Einstellung aktiviert ist. Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die nicht in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind. Diese Benutzer können unabhängig vom Status dieser Einstellung keine Verbindung zum VDA herstellen.

### ICA-Listener - Verbindungstimeout

**Hinweis:** Diese Einstellung gilt nur für Virtual Delivery Agents 5.0, 5.5 und 5.6 Feature Pack 1.

Mit dieser Einstellung geben Sie die maximale Wartezeit an, bis eine Verbindung mit dem ICA-Protokoll abgeschlossen wird.

Standardmäßig ist die maximale Wartezeit 120000 Millisekunden oder zwei Minuten.

### ICA-Listenerportnummer

Mit dieser Einstellung konfigurieren Sie die TCP/IP-Portnummer, die vom ICA-Protokoll auf dem Server verwendet wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Standardeinstellung der Portnummer ist "1494".

Gültige Portnummern müssen zwischen 0 und 65535 liegen. Sie dürfen keinen Konflikt mit anderen gängigen Portnummern verursachen. Wenn Sie die Portnummer ändern, muss der Server neu gestartet werden, damit der neue Wert wirksam werden kann. Wenn Sie die Portnummer auf dem Server ändern, müssen Sie sie auch in jedem Citrix Receiver oder Plug-In ändern, das eine Verbindung zu diesem Server herstellt.

### Starten nicht-veröffentlichter Programme bei Clientverbindung

Mit dieser Einstellung geben Sie an, ob Startanwendungen über RDP auf dem Server gestartet werden.

Standardmäßig ist das Starten von Startanwendungen über RDP auf dem Server nicht zulässig.

### Schreiben in Clientzwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Clientzwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

### Schreiben in Sitzungszwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Clientzwischenablagedaten nicht für die Benutzersitzung freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Sitzungszwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

### Zum Schreiben in Sitzungszwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Sitzungszwischenablage einschränken aktiviert ist, können Clientzwischenablagedaten nicht für Sitzungsanwendungen freigegeben werden. Mit dieser Einstellung können jedoch bestimmte Datenformate für die Sitzungszwischenablage freigegeben werden.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML-Format

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** zugelassen ist.
- Stellen Sie sicher, dass **Schreiben in Sitzungszwischenablage einschränken** aktiviert ist.
- Fügen Sie einen Eintrag für **HTML-Format** (und alle anderen Formate, die unterstützt werden sollen) unter **Zum Schreiben in Sitzungszwischenablage zugelassene Formate** hinzu.

**Hinweis:** Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (HTML-Format) werden alle vorhandenen Skripts von der Quelle des kopierten Inhalts an das Ziel kopiert. Vergewissern Sie sich vor dem Kopieren, dass eine Vertrauensstellung zur Quelle besteht. Wenn Sie Inhalte mit Skripts kopieren, werden diese nur aktiviert, wenn Sie die Zieldatei als HTML-Datei speichern und ausführen.

Zusätzliche benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung wird nicht angewendet, wenn die Einstellung Clientzwischenablagenumleitung oder Schreiben in Sitzungszwischenablage einschränken auf "Nicht zugelassen" festgelegt sind.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients"

Jul 08, 2016

Der Abschnitt "Automatische Wiederverbindung von Clients" enthält Richtlinieneinstellungen, mit denen Sie die automatische Wiederverbindung von Sitzungen steuern.

## Automatische Wiederverbindung von Clients

Diese Einstellung legt fest, ob die automatische Wiederverbindung des gleichen Clients zulässig ist, nachdem eine Verbindung unterbrochen wurde.

Standardmäßig ist die automatische Wiederverbindung zugelassen.

Ist die automatische Wiederverbindung zulässig, können Benutzer ihre Arbeit an der Stelle wiederaufnehmen, an der die Verbindung unterbrochen wurde. Die automatische Wiederverbindung erkennt unterbrochene Verbindungen und verbindet die Benutzer wieder mit ihren Sitzungen.

Bei der automatischen Wiederverbindung kann es aber dazu kommen, dass eine neue Sitzung gestartet wird (statt die Verbindung mit der bestehenden Sitzung wiederherzustellen), wenn das Citrix Receiver-Cookie, das den Schlüssel für Sitzungs-ID und Anmeldeinformationen enthält, nicht verwendet wird. Das Cookie wird nicht verwendet, wenn es abgelaufen ist, z. B. weil die Wiederverbindung verzögert wird, oder wenn die Anmeldeinformationen neu eingegeben werden müssen. Die automatische Wiederverbindung von Clients wird nicht ausgelöst, wenn Benutzer die Sitzung absichtlich trennen.

Wenn die automatische Wiederverbindung zugelassen ist, versucht Citrix Receiver bei Anwendungssitzungen, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Wenn die automatische Wiederverbindung zugelassen ist, versucht Citrix Receiver bei Desktopsitzungen eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
wobei <Sekunden> die Zeit in Sekunden ist, nach deren Ablauf keine weiteren Versuche der Sitzungswiederherstellung erfolgen.

## Authentifizierung bei automatischer Wiederverbindung von Clients

Mit dieser Einstellung ist die Authentifizierung erforderlich, wenn die Verbindung zum Client automatisch wiederhergestellt wird.

Standardmäßig ist die Authentifizierung nicht erforderlich.

Wenn sich ein Benutzer erstmals anmeldet, werden seine Anmeldeinformationen verschlüsselt und gespeichert und es wird ein Cookie mit dem Schlüssel erstellt und an Citrix Receiver gesendet. Wenn diese Einstellung konfiguriert ist, werden keine Cookies verwendet. Stattdessen wird ein Dialogfeld mit der Aufforderung zur Eingabe der Anmeldeinformationen angezeigt, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Protokollierung der automatischen Wiederverbindung von Clients

Mit dieser Einstellung legen Sie fest, ob die automatischen Wiederverbindungen im Ereignisprotokoll aufgezeichnet werden.

Standardmäßig ist die Protokollierung deaktiviert.

Wenn die Protokollierung aktiviert ist, werden Informationen über erfolgreiche und fehlgeschlagene Wiederverbindungsereignisse im Systemprotokoll des Servers aufgezeichnet. Eine Site stellt kein kombiniertes Protokoll zu Wiederverbindungsereignissen auf allen Servern zur Verfügung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Audio"

Jul 08, 2016

Der Abschnitt "Audio" enthält Richtlinieneinstellungen, mit denen Sie das Senden und Empfangen von Audiodaten auf dem Benutzergerät konfigurieren können, ohne dass es dabei zu einer unerwünschten Verschlechterung der Leistung kommt.

## Audio über UDP - Real-time Transport

Diese Einstellung aktiviert bzw. deaktiviert die Audioübertragung und den Audioempfang zwischen VDA und Benutzergeräten über RTP mit UDP (User Datagram Protocol). Wenn diese Einstellung deaktiviert ist, wird Audio über TCP gesendet und empfangen.

Standardmäßig ist Audio über UDP zugelassen.

## Audio Plug & Play

Mit dieser Einstellung lassen Sie die Verwendung mehrerer Audiogeräte zum Aufzeichnen und zum Wiedergeben von Ton zu oder verhindern sie.

Standardmäßig ist die Verwendung mehrerer Audiogeräte zulässig.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

## Audioqualität

Mit dieser Einstellung legen Sie die Tonqualität fest, die in Benutzersitzungen empfangen wird.

In der Standardeinstellung ist die Tonqualität auf Hoch - High Definition-Audio eingestellt.

Um die Tonqualität zu steuern, wählen Sie eine der folgenden Optionen:

- Wählen Sie Gering - für langsame Verbindungen für Verbindungen mit geringer Bandbreite. An das Benutzergerät gesendete Audiodaten werden bis auf 16 KBit/s komprimiert. Diese Komprimierung führt zu einer erheblichen Verringerung der Tonqualität, ermöglicht aber eine akzeptable Leistung bei einer Verbindung mit geringer Bandbreite.
- Wählen Sie Mittel - für Sprache optimiert, um VoIP-Anwendungen oder Medienanwendungen bei schwierigen Netzwerkverbindungen mit Leitungen unter 512 KBit/s oder bei erheblicher Überlastung und Paketverlust bereitzustellen. Dieses Codec bietet eine schnelle Codierung und ist daher ideal für Softphones und Unified Communications-Anwendungen geeignet, wenn Sie eine serverseitige Medienverarbeitung benötigen.
  Die an das Benutzergerät gesendeten Audiodaten werden bis auf 64 KBit/s komprimiert; diese Komprimierung führt zu einer moderaten Verringerung der Tonqualität auf dem Benutzergerät mit niedriger Latenz und geringem Bandbreitenverbrauch. Wenn die Einstellung eine unbefriedigende VoIP-Qualität liefert, stellen Sie sicher, dass die Richtlinie Audio über UDP - Real-time Transport auf Zugelassen eingestellt ist.

- Wählen Sie Hoch - High Definition Audio für Verbindungen, bei denen die Bandbreite keine Rolle spielt und bei denen die Tonqualität wichtig ist. Clients können Audiodaten mit der nativen Abspielrate wiedergeben. Audiodaten werden mit einer hohen Qualitätsstufe bei Erhaltung der CD-Qualität komprimiert, die bis zu 112 KBit/s Bandbreite benötigt. Die Übertragung dieser Datenmenge kann zu einer höheren CPU-Belastung und Engpässen im Netzwerk führen.

Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch.

Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

(Prozent), um die maximale Bandbreite anzugeben.

### Clientaudioumleitung

Mit dieser Einstellung legen Sie fest, ob auf dem Server gehostete Anwendungen Audiodateien über ein auf dem Benutzergerät installiertes Audiogerät wiedergeben können. Diese Einstellung gibt auch an, ob Benutzer Audio aufzeichnen können.

Standardmäßig ist die Audioumleitung zugelassen.

Nachdem Sie diese Einstellung zugelassen haben, können Sie die Bandbreite beschränken, die durch die Wiedergabe oder das Aufzeichnen von Audio verbraucht wird. Durch Beschränken der Bandbreite, die durch Audio verbraucht wird, kann sich die Anwendungsleistung steigern, die Audioqualität wird aber herabgesetzt. Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch. Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung (Prozent), um die maximale Bandbreite anzugeben.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wichtig: Wenn die Clientaudioumleitung nicht zugelassen ist, sind alle HDX-Audiofunktionen deaktiviert.

### Clientmikrofonumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Umleitung von Clientmikrofonen. Wenn aktiviert, können Benutzer Mikrofone für die Aufnahme von Audioeingaben in einer Sitzung verwenden.

Standardmäßig ist die Clientmikrofonumleitung zugelassen.

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Geräten haben, auf Mikrofone zugreifen. Benutzer können den Zugriff ermöglichen oder ablehnen. Benutzer können die Warnung in Citrix Receiver deaktivieren.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wenn die Einstellung Clientaudioumleitung auf dem Benutzergerät deaktiviert ist, hat diese Regel keine Auswirkung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Bandbreite"

Jul 08, 2016

Der Abschnitt "Bandbreite" enthält Richtlinieneinstellungen, mit denen Sie Leistungsprobleme vermeiden können, die sich aus der Bandbreitenverwendung in der Clientsitzung ergeben.

Wichtig: Die Verwendung dieser Richtlinieneinstellungen mit den Richtlinieneinstellungen Multistream kann zu unerwarteten Ergebnissen führen. Wenn Sie Multistreameinstellungen in einer Richtlinie verwenden, stellen Sie sicher, dass diese Richtlinieneinstellungen für das Bandbreitenlimit nicht eingeschlossen sind.

## Bandbreitenlimit für die Audioumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Wiedergabe oder die Aufnahme von Audio in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

## Bandbreitenlimit für die Audioumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für die Wiedergabe oder die Aufnahme von Audio in als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

## Bandbreitenlimit für Client-USB-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

## Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren,


© 1999-2017 Citrix Systems, Inc. All rights reserved.

mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für Zwischenablagenumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für Zwischenablagenumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für COM-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).
Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf einen COM-Port in einer Clientverbindung in Kilobits pro Sekunde an. Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung Bandbreitenlimit für COM-Portumleitung (Prozent), wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für COM-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).
Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf COM-Ports in einer Clientverbindung als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und auch für die Einstellung Bandbreitenlimit für COM-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für Dateiumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientlaufwerke in einer Clientverbindung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Dateiumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung (mit dem niedrigeren Wert) angewendet.

### Bandbreitenlimit für Dateiumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für den Zugriff auf Clientlaufwerke als Prozentsatz der Gesamtsitzungsbandbreite an

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Dateiumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung "Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung", wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für LPT-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).
Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde an, die für Druckaufträge über den LPT-Port in einer Benutzersitzung verwendet werden kann.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung Bandbreitenlimit für LPT-Portumleitung (Prozent), wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für LPT-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).
Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite, die für Druckaufträge über den LPT-Port in einer Sitzung verwendet werden darf, als Prozent der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für LPT-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für Sitzung insgesamt

Mit dieser Einstellung geben Sie Gesamtbandbreite in Kilobits pro Sekunde an, die für Benutzersitzungen verwendet werden kann.

Die maximal erzwingbare Bandbreitenbeschränkung ist 10 MBit/s (10.000 KBit/s). Standardmäßig ist kein Maximalwert (Null) angegeben.

Durch Beschränken der Bandbreite, die von einer Clientverbindung verbraucht wird, kann zu einer Leistungsverbesserung führen, wenn andere Anwendungen außerhalb der Clientverbindung auch auf die Bandbreite zugreifen.

### Bandbreitenlimit für Druckerumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für Druckerumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

### Bandbreitenlimit für TWAIN-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) einen Wert


© 1999-2017 Citrix Systems, Inc. All rights reserved.

angeben, wird die restriktivere Einstellung angewendet.

### Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Clientsensoren"

Jul 08, 2016

Der Abschnitt "Clientsensoren" enthält Richtlinieneinstellungen, mit denen gesteuert wird, wie Informationen über den Mobilgerätsensor in einer Benutzersitzung gehandhabt werden.

## Anwendungen können den physischen Standort des Clientgeräts verwenden

Diese Einstellung legt fest, ob Anwendungen, die in einer Sitzung auf einem Mobilgerät ausgeführt werden, den physischen Standort des Benutzergeräts verwenden können.

In der Standardeinstellung ist die Verwendung von Standortinformationen nicht zugelassen.

Wenn diese Einstellung nicht zugelassen ist und eine Anwendung versucht, die Standortinformationen abzurufen, wird ein Wert von "Zugriff verweigert" zurückgegeben.

Wenn diese Einstellung nicht zugelassen ist, kann ein Benutzer die Verwendung von Standortinformationen verhindern und eine Citrix Receiver-Anforderung für den Zugriff auf den Standort ablehnen. Android- und iOS-Geräte senden am Anfang jeder Sitzung eine Anforderung für die Standortinformationen.

Berücksichtigen Sie beim Entwickeln von gehosteten Anwendungen, die die Einstellung Anwendungen können den physischen Standort des Clientgeräts verwenden enthalten Folgendes:

- Eine standortaktivierte Anwendung sollte sich aus den folgenden Gründen nicht darauf verlassen, dass Standortinformationen verfügbar sind:
  - Ein Benutzer gewährt möglicherweise keinen Zugriff auf die Standortinformationen.
  - Der Standort ist ggf. nicht verfügbar oder ändert sich, währen die Anwendung ausgeführt wird.
  - Ein Benutzer stellt möglicherweise eine Verbindung mit der Anwendungssitzung von einem anderen Gerät her, das keine Standortinformationen unterstützt.
- Anforderungen für eine standortaktivierte Anwendung:
  - Das Standortfeature muss in der Standardeinstellung deaktiviert sein.
  - Eine Benutzeroption für das Zulassen oder Ablehnen des Features muss bei Ausführung der Anwendung verfügbar sein.
  - Eine Benutzeroption muss verfügbar sein, mit der von der Anwendung zwischengespeicherte Standortdaten gelöscht werden. (Citrix Receiver speichert keine Standortdaten im Cache.)
- Eine standortaktivierte Anwendung muss die Granularität der Standortinformationen verwalten, damit die abgefragten Daten dem Zweck der Anwendung entsprechen und die entsprechenden Gesetze einhalten.
- Bei der Verwendung der Standortdienste sollte eine sichere Verbindung (zum Beispiel mit TLS oder einem VPN) erzwungen werden. Citrix Receiver sollte eine Verbindung mit vertrauenswürdigen Servern herstellen.
- Sie sollten eine Rechtsberatung hinsichtlich der Verwendung von Standortdiensten erwägen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Desktopbenutzeroberfläche"

Aug 17, 2016

Der Abschnitt "Desktopbenutzeroberfläche" enthält Richtlinieneinstellungen für visuelle Effekte, wie Desktophintergrund, Menüanimationen und das Verhalten von Fensterinhalten beim Drag & Drop, um die für Clientverbindungen verbrauchte Bandbreite zu steuern. Die Anwendungsleistung über ein WAN lässt sich durch Beschränken des Bandbreitenverbrauchs verbessern.

## Desktopgestaltungsumleitung

Mit dieser Einstellung geben Sie an, ob die Verarbeitung des Grafikprozessors (GPU) oder des integrierten Grafikprozessors (IGP) auf dem Benutzergerät für die lokale DirectX-Grafikwiedergabe verwendet werden soll, um eine nahtlosere Windows-Desktopdarstellung zu erzielen. Wenn die Desktopgestaltungsumleitung aktiviert ist, wird eine hoch reaktionsfähige Windows-Benutzererfahrung bei Beibehaltung einer hohen Skalierbarkeit auf dem Server gewährleistet.

Standardmäßig ist die Desktopgestaltungsumleitung deaktiviert.

Um die Desktopgestaltungsumleitung auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie Deaktiviert aus, wenn Sie diese Einstellung einer Richtlinie möchten.

## Grafikqualität Desktopgestaltung

Mit dieser Einstellung wird die Qualität der für die Desktopgestaltungsumleitung verwendeten Grafiken angegeben.

Die Standardeinstellung ist "Hoch".

Wählen Sie die Qualität Hoch, Mittel, Niedrig oder Verlustfrei aus.

## Desktophintergrund

Mit dieser Einstellung legen Sie fest, ob Hintergründe in Benutzersitzungen angezeigt werden.

Standardmäßig kann der Desktophintergrund in Benutzersitzungen angezeigt werden.

Um den Desktophintergrund auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie die Einstellung Nicht zugelassen, wenn Sie diese Einstellung einer Richtlinie hinzufügen.

## Menüanimation

Mit dieser Einstellung legen Sie fest, ob Menüanimation in Benutzersitzungen zugelassen oder verhindert wird.

Standardmäßig ist Menüanimation zugelassen.

Menüanimation ist eine Microsoft-Einstellung für erleichterte Bedienung. Ist die Einstellung aktiviert, werden Menüs nach einer kurzen Verzögerung durch Bildlauf- oder Einblendeffekt angezeigt. Unten im Menü wird ein Pfeil angezeigt. Das Menü wird eingeblendet, wenn Sie mit der Maus auf diesen Pfeil zeigen.

Menüanimation ist auf einem Desktop aktiviert, wenn diese Richtlinieneinstellung auf Zugelassen festgelegt ist und die Microsoft-Einstellung für Menüanimation aktiviert ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Änderungen an der Microsoft-Einstellung für Menüanimation sind Desktopänderungen. Dies bedeutet, dass einem Benutzer, der Menüanimation in einer Sitzung aktiviert hat, in späteren Sitzungen auf dem Desktop keine Menüanimation zur Verfügung steht, wenn die Desktopeinstellungen so festgelegt sind, dass am Desktop vorgenommene Änderungen nach dem Beenden der Sitzung verworfen werden. Aktivieren Sie daher für Benutzer, die Menüanimation benötigen, die Microsoft-Einstellung im Masterimage für den Desktop oder stellen Sie sicher, dass der Desktop vom Benutzer vorgenommene Änderungen beibehält.

### Fensterinhalt beim Verschieben anzeigen

Mit dieser Einstellung legen Sie fest, ob Fensterinhalte beim Verschieben des Fensters auf dem Bildschirm angezeigt werden.

Standardmäßig ist die Anzeige des Fensterinhalts beim Verschieben zugelassen.

Wenn Zugelassen ausgewählt ist, wird beim Verschieben das ganze Fenster angezeigt. Wenn Nicht zugelassen ausgewählt ist, wird bis zum Ablegen nur der Fensterrahmen beim Verschieben angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Endbenutzerüberwachung"

Jul 08, 2016

Der Abschnitt "Endbenutzerüberwachung" enthält Richtlinien zum Messen von Sitzungsnetzwerkverkehr.

## ICA-Roundtripberechnung

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für aktive Verbindungen durchgeführt werden.

Standardmäßig sind die Berechnungen für aktive Verbindungen aktiviert.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist

## Intervall für ICA-Roundtripberechnung

Mit dieser Einstellung geben Sie die Häufigkeit an, in Sekunden, mit der ICA-Roundtripberechnungen durchgeführt werden

Standardmäßig wird der ICA-Roundtrip alle 15 Sekunden berechnet.

## ICA-Roundtrip für Verbindungen im Leerlauf berechnen

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für Verbindungen im Leerlauf durchgeführt werden.

Standardmäßig werden Berechnungen nicht für Verbindungen im Leerlauf durchgeführt.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Richtlinieneinstellung für Enhanced Desktop Experience

Jul 08, 2016

Durch die Richtlinieneinstellung "Enhanced Desktop Experience" werden Sitzungen auf Serverbetriebssystemen so konfiguriert, dass sie wie lokale Windows 7-Desktops aussehen, damit Benutzer in den Genuss einer verbesserten Desktopdarstellung kommen.

Standardmäßig ist diese Einstellung zugelassen.

Wenn ein Benutzerprofil mit dem Design "Windows – klassisch" bereits auf dem virtuellen Desktop vorhanden ist, wird durch Aktivieren dieser Richtlinie nicht die verbesserte Desktopdarstellung für diesen Benutzer bereitgestellt. Wenn sich ein Benutzer, dessen Benutzerprofil mit einem Windows 7-Design konfiguriert ist, bei einem virtuellen Desktop unter Windows Server 2012 anmeldet, für den diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird eine Fehlermeldung angezeigt, die angibt, dass das Design nicht angewendet werden kann.

In beiden Fällen kann das Problem durch Zurücksetzen des Benutzerprofils gelöst werden.

Wenn die Richtlinie auf einem virtuellen Desktop mit aktiven Benutzersitzungen deaktiviert wird, sind Aussehen und Verhalten von Sitzungen nicht mit der Desktopdarstellung von Windows 7 und Windows - klassisch konsistent. Wenn Sie dies vermeiden möchten, starten Sie den virtuellen Desktop neu, nachdem Sie die Richtlinieneinstellung geändert haben. Sie müssen auch sämtliche Roamingprofile auf dem virtuellen Desktop löschen. Citrix empfiehlt außerdem, alle anderen Benutzerprofile auf dem virtuellen Desktop zu löschen, um Inkonsistenzen zwischen Profilen zu vermeiden.

Wenn Sie Roamingbenutzerprofile in der Umgebung verwenden, stellen Sie sicher, dass das Feature "Enhanced Desktop Experience" für alle virtuellen Desktops, die sich ein Profil teilen, entweder aktiviert oder deaktiviert ist.

Citrix rät davon ab, Roamingprofile zwischen virtuellen Desktops, auf denen Serverbetriebssysteme und Clientbetriebssysteme ausgeführt werden, freizugeben. Die Profile für Client- und Serverbetriebssysteme sind unterschiedlich und das Freigeben von Roamingprofilen zwischen beiden Systemtypen kann zu Inkonsistenzen in den Profileigenschaften führen, wenn ein Benutzer zwischen den Systemen wechselt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Dateiumleitung"

Jul 08, 2016

Der Abschnitt "Dateiumleitung" enthält Richtlinieneinstellungen für die Clientlaufwerkzuordnung und die Clientlaufwerkoptimierung.

## Clientlaufwerke automatisch verbinden

Mit dieser Einstellung legen Sie fest, ob die automatische Verbindung von Clientlaufwerken bei der Benutzeranmeldung zugelassen ist.

In der Standardeinstellung ist die automatische Verbindung zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellungen für die Laufwerktypen aktivieren, die automatisch verbunden werden. Konfigurieren Sie beispielsweise Optische Clientlaufwerke, damit CD-Laufwerke auf dem Clientgerät automatisch verbunden werden.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientlaufwerkumleitung
- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

## Clientlaufwerkumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Dateiumleitung von und zu Laufwerken auf dem Benutzergerät.

In der Standardeinstellung ist die Dateiumleitung aktiviert.

Wenn aktiviert, können Benutzer ihre Dateien auf allen Clientlaufwerken speichern. Wenn deaktiviert, wird jegliche Dateiumleitung verhindert, unabhängig von den Dateiumleitungseinstellungen für einzelne Laufwerkstypen, z. B. Clientdiskettenlaufwerke und Clientnetzlaufwerke.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

## Lokale Clientfestplattenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die lokalen Festplattenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf lokale Festplattenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können lokale Festplattenlaufwerke nicht


© 1999-2017 Citrix Systems, Inc. All rights reserved.

zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Lokale Festplattenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit lokale Festplattenlaufwerke automatisch verbunden werden.

### Clientdiskettenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die Diskettenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf Diskettenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Diskettenlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientdiskettenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Diskettenlaufwerke automatisch verbunden werden.

### Clientnetzlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die (remoten) Netzlaufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Netzlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Netzlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientnetzlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Netzlaufwerke automatisch verbunden werden.

### Optische Clientlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf CD-, DVD- und BD-Laufwerke des Clientgeräts zugreifen oder Dateien dort speichern können.

In der Standardeinstellung ist der Zugriff auf optische Clientlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können optische Clientlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Optische Clientlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit optische Clientlaufwerke automatisch verbunden werden.

### Clientwechsellaufwerke

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die USB-Laufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Clientwechsellaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Clientwechsellaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientwechsellaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Clientwechsellaufwerke automatisch verbunden werden.

### Host-zu-Client-Umleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Dateitypzuordnungen für URLs und manche Medieninhalte, damit sie auf dem Clientgerät geöffnet werden. Wenn deaktiviert, werden Inhalte auf dem Server geöffnet.

In der Standardeinstellung ist die Dateitypzuordnung deaktiviert.

Diese Art von URLs werden lokal geöffnet, wenn Sie die Einstellung aktivieren:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player und QuickTime (RTSP)
- Real Player und QuickTime (RTSPU)
- Ältere Real Player-URLs (PNM)
- Microsoft Media Server (MMS)

### Clientlaufwerksbuchstaben erhalten

Mit dieser Einstellung aktivieren oder deaktivieren Sie, ob die Clientlaufwerksbuchstaben erhalten bleiben.

In der Standardeinstellung bleiben die Clientlaufwerksbuchstaben nicht erhalten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

### Schreibgeschützter Zugriff auf Clientlaufwerke

Diese Einstellung erlaubt oder verhindert, dass Benutzer und Anwendungen Dateien oder Ordner auf zugeordneten Clientlaufwerken erstellen oder ändern.

Standardmäßig können Dateien und Ordner auf zugeordneten Clientlaufwerken geändert werden.

Wenn die Einstellung auf Aktiviert gesetzt wird, ist Lesezugriff auf die Dateien und Verzeichnisse möglich.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

### Umleitung spezieller Ordner

Mit dieser Einstellung legen Sie fest, ob Benutzer von Citrix Receiver und dem Webinterface ihre lokalen speziellen Ordner in einer Sitzung sehen, z. B. "Dokumente" und "Desktop".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

In der Standardeinstellung ist die Umleitung spezieller Ordner zugelassen.

Diese Einstellung verhindert, dass jegliche Objekte, die durch eine Richtlinie gefiltert werden, die Umleitung spezieller Ordner verwenden. Einstellungen an anderer Stelle werden nicht beachtet. Wenn diese Einstellung nicht zugelassen ist, werden verwandte Einstellungen im Webinterface, in StoreFront oder Citrix Receiver ignoriert.

Sie legen fest, welche Benutzer die Umleitung spezieller Ordner erhalten, indem Sie Zugelassen wählen und diese Einstellung in eine Richtlinie aufnehmen, die nach den Benutzern gefiltert wird, denen diese Funktion zur Verfügung stehen soll. Diese Einstellung überschreibt alle anderen Einstellungen für die Umleitung spezieller Ordner.

Die Umleitung spezieller Ordner interagiert mit dem Clientgerät. Daher verhindern Einstellungen, die den Benutzerzugriff auf lokale Festplatten untersagen, auch die Umleitung spezieller Ordner.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Lokale Clientfestplattenlaufwerke die Option Zugelassen wählen.

### Asynchrones Schreiben verwenden

Mit dieser Einstellung aktivieren oder deaktivieren Sie asynchrones Schreiben auf Laufwerke.

Standardmäßig ist das asynchrone Schreiben deaktiviert.

Für Verbindungen über WANs, die normalerweise durch relativ hohe Bandbreite und hohe Latenz charakterisiert sind, können Sie durch asynchrone Schreibvorgänge die Dateiübertragungen und Schreibvorgänge auf Clientlaufwerke beschleunigen. Sollte jedoch ein Verbindungsfehler oder Datenträgerfehler auftreten, können die Clientdateien, die geschrieben werden, in einem nicht definierten Zustand enden. Dem Benutzer werden dann in einem Popupfenster die betroffenen Dateien angezeigt. Der Benutzer kann das Problem beheben, z. B. durch Neustart einer unterbrochenen Dateiübertragung bei der Wiederverbindung oder nach Beheben eines Datenträgerfehlers.

Citrix empfiehlt, dass asynchrone Schreibvorgänge auf Datenträgern nur für Benutzer implementiert werden, die eine Remoteverbindung mit guter Geschwindigkeit für die Dateiübertragungen benötigen, und die verlorene Dateien oder Daten problemlos wiederherstellen können, sollten Fehler bei der Verbindung oder dem Datenträger auftreten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellung deaktiviert ist, finden keine asynchronen Schreibvorgänge statt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Flash-Umleitung"

Jul 08, 2016

Der Abschnitt "Flash-Umleitung" enthält Richtlinieneinstellungen für die Behandlung von Flash-Inhalten in Benutzersitzungen.

## Flash-Beschleunigung

Aktiviert oder deaktiviert die Wiedergabe von Flash-Inhalten auf Benutzergeräten statt auf dem Server. Standardmäßig ist die clientseitige Wiedergabe von Flash-Inhalten aktiviert.

Hinweis: Diese Einstellung wird für die Legacy-Flash-Umleitung mit dem Citrix Online Plug-In 12.1 verwendet.
Wenn aktiviert, reduziert diese Einstellung die Netzwerk- und Serverlast, indem Flash-Inhalte auf dem Clientgerät wiedergegeben werden. Zusätzlich erreichen Sie mit der Einstellung Flash-URL-Kompatibilitätsliste, dass Flash-Inhalte von bestimmten Websites auf dem Server wiedergegeben werden.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Ist diese Einstellung deaktiviert, werden Flash-Inhalte von allen Websites, unabhängig von deren URLs, auf dem Server wiedergegeben. Damit nur die Flash-Inhalte bestimmter Websites auf dem Benutzergerät wiedergeben werden, konfigurieren Sie die Einstellung Flash-URL-Kompatibilitätsliste.

## Flash-Hintergrundfarbenliste

Mit dieser Einstellung können Sie Schlüsselfarben für bestimmte URLs festlegen.

In der Standardeinstellung sind keine Schlüsselfarben angegeben.

Schlüsselfarben werden hinter clientseitig wiedergegebenem Flash angezeigt und unterstützen die visuelle Erkennung von Bereichen. Die angegebene Schlüsselfarbe sollte selten sein, sonst funktioniert die visuelle Bereichserkennung ggf. nicht richtig.

Gültige Eingaben bestehen aus einer URL (mit optionalen Platzhaltern am Anfang und Ende), der ein 24-Bit-RGB-Farbhexcode folgt. Zum Beispiel: http://citrix.com 000003.

Stellen Sie sicher, dass die angegebene URL die URL für den Flash-Inhalt ist. Sie weicht möglicherweise von der URL der Website ab.

> **Warnung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Auf VDA-Maschinen, auf denen Windows 8 oder Windows 2012 ausgeführt wird, werden mit dieser Einstellung möglicherweise nicht die Schlüsselfarben für die URL festgelegt. Wenn dieses Problem auftritt, bearbeiten Sie die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registrierung auf der VDA-Maschine.

Verwenden Sie bei 32-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Verwenden Sie bei 64-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

### Flash-Abwärtskompatibilität

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung von Originalfeatures für die Legacy-Flash-Umleitung mit älteren Versionen von Citrix Receiver (früher Citrix Online Plug-In).

Standardmäßig ist diese Einstellung aktiviert.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Flash-Umleitungsfeatures der zweiten Generation können mit Citrix Receiver 3.0 verwendet werden. Legacyumleitungsfeatures werden mit dem Citrix Online Plug-In 12.1 unterstützt. Um sicherzustellen, dass die Flash-Umleitungsfeatures der zweiten Generation verwendet werden, muss die Flash-Umleitung der zweiten Generation auf dem Server und dem Benutzergerät aktiviert sein. Wenn die Legacyumleitung entweder auf dem Server oder dem Benutzergerät aktiviert ist, werden die Legacyumleitungsfeatures verwendet.

### Flash-Standardverhalten

Mit dieser Einstellung wird das Standardverhalten für die Flash-Beschleunigung der zweiten Generation festgelegt.

Standardmäßig ist die Flash-Beschleunigung aktiviert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- Flash-Beschleunigung aktivieren: Flash-Umleitung wird verwendet.
- Flash Player blockieren: Flash-Umleitung sowie serverseitige Wiedergabe werden nicht verwendet. Der Benutzer kann keine Flash-Inhalte anzeigen.
- Flash-Beschleunigung deaktivieren: Flash-Umleitung wird nicht verwendet. Der Benutzer kann auf dem Server wiedergegebene Flash-Inhalte anzeigen, wenn ein mit den Inhalten kompatibler Adobe Flash Player für Windows Internet Explorer auf dem Server installiert ist.

Diese Einstellung kann für einzelne Webseiten und Flash-Instanzen basierend auf der Einstellung Flash-URL-Kompatibilitätsliste überschrieben werden. Außerdem muss auf dem Benutzergerät die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren aktiviert sein.

### Flash-Ereignisprotokollierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Aufzeichnung von Flash-Ereignissen im Windows-Anwendungsereignisprotokoll.

Standardmäßig ist die Protokollierung aktiviert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Auf Computern unter Windows 7 oder Windows Vista wird ein spezielles Protokoll für die Flash-Umleitung im Knoten "Anwendungs- und Dienstprotokolle" angezeigt.

### Flash - intelligentes Fallback

Mit dieser Einstellung aktivieren oder deaktivieren Sie automatische Versuche, das serverseitige Rendering für Flash Player-Instanzen zu verwenden, wenn das clientseitige Rendering entweder unnötig ist oder eine schlechte Benutzererfahrung ergibt.

Standardmäßig ist diese Einstellung aktiviert.

### Flash-Latenzschwellenwert

Mit dieser Einstellung geben Sie einen Schwellenwert zwischen 0-30 Millisekunden an, um festzulegen, wo Adobe Flash-Inhalte wiedergegeben werden.

In der Standardeinstellung ist der Schwellenwert 30.

Beim Start wird die aktuelle Latenz zwischen Server und Benutzergerät von HDX MediaStream für Flash gemessen. Wenn die Latenz unter dem Schwellenwert liegt, werden Flash-Inhalte mit HDX MediaStream für Flash auf dem Benutzergerät wiedergegeben. Wenn die Latenz den Schwellenwert überschreitet, werden die Inhalte auf dem Netzwerkserver wiedergegeben, wenn Adobe Flash Player dort vorhanden ist.

Wenn Sie diese Einstellung aktivieren, muss die Einstellung Flash-Abwärtskompatibilität vorhanden und auf Zugelassen eingestellt sein.

Hinweis: Dies gilt nur, wenn HDX MediaStream Flash-Umleitung im Legacymodus verwendet wird.

### Verhindern von Flash-Videofallback

Mit dieser Einstellung geben Sie an, ob und wie "kleine" Flash-Inhalte gerendert und angezeigt werden.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Nur kleiner Inhalt:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **Nur kleiner Inhalt mit einem unterstützten Client:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, wenn der Client aktuell die Flash-Umleitung verwendet, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **Kein serverseitiger Inhalt:** Alle Inhalte auf dem Server werden durch eine Fehler-SWF-Datei ersetzt.

Zum Verwenden dieser Richtlinieneinstellung geben Sie eine Fehler-SWF-Datei an. Diese Fehler-SWF-Datei ersetzt alle Flash-Inhalte, die nicht auf dem VDA gerendert werden sollen.

### Fehler beim Verhindern von Flash-Videofallback *.swf

Diese Einstellung legt die URL der Fehlermeldung fest, die anstelle von Flash-Instanzen angezeigt wird, wenn Server-Lastverwaltungsrichtlinien verwendet werden. Beispiel:

http://domainName.tld/sample/path/error.swf

### URL-Liste für serverseitigen Flash-Inhaltsabruf


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung geben Sie die Websites an, deren Flash-Inhalte auf den Server heruntergeladen und dann auf das Benutzergerät zur Wiedergabe übertragen werden.

In der Standardeinstellung sind keine Sites angegeben.

Diese Einstellung wird verwendet, wenn das Benutzergerät keinen direkten Internetzugang hat; der Server stellt die Verbindung bereit. Auf dem Benutzergerät muss die Einstellung Serverseitigen Inhaltsabruf aktivieren auch aktiviert sein.

Die Flash-Umleitung der zweiten Generation enthält ein Fallback für den serverseitigen Flash-Inhaltsabruf für SWF-Dateien. Wenn ein Benutzergerät keine Flash-Inhalte von einer Website abrufen kann und die Website in der URL-Liste für serverseitigen Flash-Inhaltsabruf aufgeführt ist, erfolgt der serverseitige Inhaltsabruf automatisch.

Hinzufügen von URLs zur Liste:

- Fügen Sie die URL der Flash-Anwendung und nicht die HTML-Seite auf oberster Ebene hinzu, die Flash Player initiiert.
- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um alle untergeordneten URLs zuzulassen (http://www.citrix.com/*).
- Die Präfixe http:// und https:// werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.

### Flash-URL-Kompatibilitätsliste

Mit dieser Einstellung geben Sie die Regeln an, die festlegen, ob die Wiedergabe von Flash-Inhalten auf bestimmten Websites auf dem Benutzergerät oder auf dem Server erfolgt oder ob sie blockiert wird.

In der Standardeinstellung sind keine Regeln angegeben.

Hinzufügen von URLs zur Liste:

- Sortieren Sie die Liste nach Priorität, sodass die wichtigsten URLs, Aktionen und Wiedergabeorte ganz oben stehen.
- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um auf alle untergeordneten URLs zu verweisen (http://www.citrix.com/*).
- Die Präfixe http:// und https:// werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.
- Fügen Sie der Liste Websites hinzu, deren Flash-Inhalte nicht richtig auf dem Benutzergerät wiedergegeben werden, und wählen Sie entweder die Optionen Auf Server rendern oder Blockieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Grafiken"

Jul 08, 2016

Der Abschnitt "Grafiken" enthält Richtlinieneinstellungen, mit denen Sie steuern, wie Bilder in Benutzersitzungen behandelt werden.

## Visuell verlustfreie Komprimierung zulassen

Mit dieser Einstellung wird für Grafiken visuell verlustfreie Komprimierung statt echter verlustfreier Komprimierung verwendet. Visuell verlustfreie Komprimierung steigert im Vergleich zu echter verlustfreier Komprimierung die Leistung, hat jedoch geringe Verluste, die für das Auge nicht erkennbar sind. Durch diese Einstellung ändert sich die Verwendung der Einstellungswerte für die visuelle Qualität.

Diese Einstellung ist standardmäßig deaktiviert.

## Anzeigespeicherlimit

Mit dieser Einstellung geben Sie die maximale Größe des Videopuffers (in Kilobytes) für die Sitzung an.

Das Standardlimit ist 65536 Kilobytes.

Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Berechnen Sie den maximal erforderlichen Arbeitsspeicher mit dieser Formel:

Speicher in Byte = (Farbtiefe in Bits pro Pixel) / 8) * (vertikale Auflösung in Pixel)*(horizontale Auflösung in Pixel).

Beispiel: Bei einer Farbtiefe von 32, einer vertikalen Auflösung von 600 und einer horizontalen Auflösung von 800 ergibt dies einen maximal erforderlichen Arbeitsspeicher von (32 / 8) * (600) * (800) = 1920000 Byte, was ein Anzeigespeicherlimit von 1920 KB ergibt.

Andere Farbtiefen als 32 Bit sind nur verfügbar, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

HDX weist Benutzern nur den pro Sitzung erforderlichen Anzeigespeicher zu. Wenn also nur einige Benutzer mehr als den Standardspeicher benötigen, hat das Erhöhen des Anzeigespeicherlimits keine negativen Auswirkungen auf die Skalierbarkeit.

## Herabsetzungspräferenz für Anzeigemodus

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Diese Einstellung gibt an, ob die Farbtiefe oder die Auflösung zuerst herabgesetzt werden soll, wenn das Speicherlimit für die Sitzung erreicht wird.

Standardmäßig wird die Farbtiefe zuerst herabgesetzt.

Wenn das Speicherlimit der Sitzung erreicht wird, können Sie die Bildqualität verringern, indem Sie erst die Farbtiefe oder erst die Auflösung herabsetzen. Wird erst die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt. Wird erst die Auflösung herabgesetzt, werden Bilder mit weniger Pixel pro Zoll angezeigt.

Wenn Benutzer in dem Fall benachrichtigt werden sollen, dass entweder die Farbtiefe oder die Auflösung herabgesetzt werden muss, konfigurieren Sie die Einstellung Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Dynamische Fenstervorschau

Mit dieser Einstellung kann die Anzeige von Seamlessfenster in den Fenstervorschaumodi Flip, Flip 3D, Taskleistenvorschau und Einsehen aktiviert bzw. deaktiviert werden.

| Windows Aero-Vorschauoption | Beschreibung |
|---|---|
| Symbolleistenvorschau | Wenn der Benutzer auf das Symbol eines Fensters zeigt, wird ein Bild dieses Fensters über der Symbolleiste angezeigt. |
| Fenstervorschau | Wenn der Benutzer auf ein Symbolleistenvorschaubild zeigt, wird das Bild in voller Größe auf dem Bildschirm angezeigt. |
| Flip | Wenn der Benutzer Alt + Tab drückt, werden kleine Vorschausymbole für jedes geöffnete Fenster angezeigt. |
| Flip-3D | Wenn der Benutzer die Tabulator- und Windows-Tasten drückt, werden große Bilder der geöffneten Fenster überlappend auf dem Bildschirm angezeigt. |

Standardmäßig ist diese Einstellung aktiviert.

### Bildzwischenspeicherung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung aktivieren oder deaktivieren Sie das Zwischenspeichern und Abrufen von Bildabschnitten in Sitzungen. Durch das Zwischenspeichern von Bildern in Abschnitten und das Abrufen dieser Abschnitte wird das Ruckeln beim Bildlauf verringert. Darüber hinaus werden weniger Daten über das Netzwerk übertragen und die Verarbeitung auf dem Benutzergerät wird reduziert.

Standardmäßig ist die Einstellung für die Bildzwischenspeicherung aktiviert.

Hinweis: Die Einstellung für die Bildzwischenspeicherung steuert, wie Bilder zwischengespeichert und abgerufen werden, jedoch nicht, ob sie zwischengespeichert werden. Wenn die Einstellung "Legacygrafikmodus" aktiviert ist, werden Bilder zwischengespeichert.

### Legacygrafikmodus

Diese Einstellung deaktiviert die umfassende Grafikdarstellung und verwendet den Legacygrafikmodus, um die Skalierbarkeit über ein WAN oder eine mobile Verbindung zu verbessern.

Die Einstellung ist standardmäßig deaktiviert und die umfassende Grafikdarstellung wird verwendet.

Der Legacygrafikmodus wird für VDAs unter Windows 7 und Windows Server 2008 R2 unterstützt. Der Modus wird zwar auch für Windows 2012 und 2012 R2 unterstützt, er wird jedoch nicht empfohlen.

Der Legacygrafikmodus wird nicht für Windows 10, 8.1 oder 8 unterstützt.

Weitere Informationen zum Optimieren von Grafikmodi und Richtlinien in XenApp und XenDesktop 7.6 FP3 oder höher finden Sie unter CTX202687.

### Maximal zugelassene Farbtiefe


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung geben Sie die maximale Farbtiefe an, die für eine Sitzung zulässig ist.

Die Standardeinstellung für die maximal zulässige Farbtiefe ist 32 Bits pro Pixel.

Diese Einstellung gilt nur für ThinWire-Treiber und -Verbindungen. Sie gilt nicht für VDAs mit einem anderen Treiber als ThinWire für die primäre Anzeige, z. B. VDAs mit WDDM-Treiber (Windows Display Driver Model). Bei Desktopbetriebssystem-VDAs mit einem WDDM-Treiber als primären Anzeigetreiber, z. B. Windows 8, hat diese Einstellung keine Auswirkung. Bei Windows-Serverbetriebssystem-VDAs mit WDDM-Treiber, z. B. Windows Server 2012 R2, kann diese Einstellung verhindern, dass Benutzer eine Verbindung mit dem VDA herstellen.

Für eine hohe Farbtiefe ist mehr Speicher erforderlich. Damit die Farbtiefe herabgesetzt wird, wenn das Speicherlimit erreicht wurde, konfigurieren Sie die Einstellung Herabsetzungspräferenz für Anzeigemodus. Wird die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt.

### Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung erzielen Sie, dass Benutzer eine kurze Erklärung erhalten, wenn die Farbtiefe oder die Auflösung herabgesetzt wird.

Standardmäßig werden Benutzer nicht benachrichtigt.

### Warteschlange und Verwerfen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung werden Bilder in der Warteschlange verworfen, die durch ein anderes Bild ersetzt wurden.

Standardmäßig ist diese Einstellung aktiviert.

Dies verbessert die Reaktionszeit, wenn Grafiken an das Benutzergerät gesendet werden. Wenn Sie diese Einstellung konfigurieren, ruckeln Animationen möglicherweise, weil Frames ausgelassen werden.

### Verwenden von Videocodec für die Komprimierung

Ermöglicht die Verwendung eines Videocodecs zum Komprimieren von Grafiken, wenn am Endpunkt eine Videodecodierung verfügbar ist. Ist am Endpunkt keine Videodecodierung verfügbar oder wenn Siefestlegen, dass kein Videocodec verwendet werden soll, wird eine Kombination aus Standbildkomprimierung und Bitmapcaching verwendet. Wenn **Bevorzugt Videocodec verwenden** ausgewählt ist, trifft das System basierend auf verschieden Faktoren die Auswahl. Die Ergebnisse variieren u. U. zwischen den Versionen, da die Auswahlmethode verbessert wird.

Wählen Sie **Videocodec nicht verwenden**, um die Server-CPU-Last zu optimieren und wenn nicht viel auf dem Server gerenderter Videoinhalt oder andere grafisch intensive Anwendungen verwendet werden.

Wählen Sie **Videocodec verwenden, wenn verfügbar**, um die Benutzererfahrung und Bandbreite zu optimieren, besonders bei viel Videoinhalt, der auf dem Server gerendert wird, und vielen 3D-Grafiken.

Wählen Sie **Bevorzugt Videocodec verwenden**, damit das System die geeignete Einstellung für das aktuelle Szenario wählt.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Die Standardeinstellung ist "Bevorzugt Videocodec verwenden".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Zwischenspeichern"

Jul 08, 2016

Der Abschnitt "Zwischenspeichern" enthält Einstellungen, mit denen Bilddaten auf Benutzergeräten zwischengespeichert werden können, wenn Clientverbindungen eine beschränkte Bandbreite haben.

## Schwellenwert für permanenten Cache

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung werden Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert. Dies ermöglicht eine Wiederverwendung von großen, oft verwendeten Bildern aus früheren Sitzungen.

Der Standardschwellenwert ist 3000000 Bits pro Sekunde.

Der Schwellenwert ist der Wert, unter dem das Feature "Permanentcache" angewendet wird. Beispielsweise werden mit dem Standardwert Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert, wenn die Bandbreite unter 3000000 Bit/s fällt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Framehawk-Richtlinieneinstellungen

Jul 08, 2016

Der Abschnitt "Framehawk" enthält Richtlinieneinstellungen zum Aktivieren und Konfigurieren des Framehawk-Anzeigekanals auf dem Server.

# Framehawk-Anzeigekanal

Wenn diese Option aktiviert ist, versucht der Server, den Framehawk-Anzeigekanal für die Grafiken und das Eingabe-Remoting der Benutzer zu verwenden. Bei diesem Anzeigekanal bietet durch UDP eine bessere Benutzererfahrung in Netzwerken mit hohem Verlust und hoher Latenz, er verbraucht jedoch u. U. mehr Serverressourcen und Bandbreite als andere Grafikmodi.

Standardmäßig ist der Framehawk-Anzeigekanal deaktiviert.

# Portbereich für Framehawk-Anzeigekanal

Mit dieser Richtlinieneinstellung geben Sie den Bereich der Portnummern an (im Format *niedrigste Portnummer,höchste Portnummer*), die vom VDA zum Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet werden. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

Der Standardportbereich ist 3224,3324.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Keep-Alive"

Jul 08, 2016

Der Abschnitt "Keep-Alive" enthält Richtlinieneinstellungen für die Verwaltung der ICA-Keep-Alive-Meldungen.

## ICA-Keep-Alive - Timeout

Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden ICA-Keep-Alive-Meldungen an.

Das Standardintervall zwischen Keep-Alive-Meldungen ist 60 Sekunden.

Geben Sie ein Intervall zwischen 1-3600 Sekunden an, in dem ICA-Keep-Alive-Meldungen gesendet werden. Konfigurieren Sie diese Einstellung nicht, wenn Sie eine Netzwerküberwachungssoftware zum Schließen inaktiver Verbindungen verwenden.

## ICA-Keep-Alives

Mit dieser Einstellung legen Sie fest, ob ICA-Keep-Alive-Meldungen in regelmäßigen Abständen gesendet werden sollen.

Standardmäßig werden keine Keep-Alive-Meldungen gesendet.

Wenn Sie diese Einstellung aktivieren, wird verhindert, dass unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität feststellt, verhindert diese Einstellung, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Meldungen, um zu ermitteln, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

ICA-Keep-Alive funktioniert nicht, wenn Sie die Sitzungszuverlässigkeit verwenden. Konfigurieren Sie daher ICA-Keep-Alive nur für Verbindungen, die die Sitzungszuverlässigkeit nicht verwenden.

Verwandte Richtlinieneinstellungen: Sitzungszuverlässigkeit - Verbindungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Lokaler App-Zugriff"

Jul 08, 2016

Der Abschnitt "Lokaler App-Zugriff" enthält Richtlinieneinstellungen, mit denen Sie die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung konfigurieren können.

## Lokalen App-Zugriff zulassen

Mit dieser Einstellung legen Sie fest, ob die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung zugelassen oder verweigert werden soll.

Wenn ein Benutzer eine lokal installierte Anwendung startet, wirkt es so, als ob diese auf dem virtuellen Desktop des Benutzers ausgeführt würde, obwohl sie tatsächlich lokal ausgeführt wird.

Standardmäßig ist der lokale App-Zugriff nicht zulässig.

## URL-Umleitungssperrliste

Mit dieser Einstellung geben Sie Websites an, die Ziel einer Weiterleitung sind und im lokalen Webbrowser gestartet werden sollen. Dies kann auch Websites umfassen, für die Gebietsschema-Informationen erforderlich sind (z. B. msn.com oder newsgoogle.com) oder Websites mit reichhaltigen Medieninhalten, die besser auf dem Benutzergerät wiedergegeben werden.

In der Standardeinstellung sind keine Sites angegeben.

## URL-Umleitungspositivliste

Mit dieser Einstellung geben Sie die Websites an, die in der Umgebung, in der sie gestartet werden, wiedergegeben werden sollen.

In der Standardeinstellung sind keine Sites angegeben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Mobilerfahrung"

Jul 08, 2016

Der Abschnitt "Mobilerfahrung" enthält Richtlinieneinstellungen für die Handhabung des Citrix Mobility Packs.

## Automatische Anzeige der Tastatur

Diese Einstellung aktiviert oder deaktiviert die automatische Anzeige der Tastatur auf Bildschirmen von Mobilgeräten.

Standardmäßig ist die automatische Anzeige der Tastatur deaktiviert.

## Für Fingereingabe optimierten Desktop starten

Diese Einstellung ist deaktiviert und für Windows 10-Maschinen nicht verfügbar.

Diese Einstellung bestimmt das allgemeine Verhalten der Citrix Receiver-Benutzeroberfläche, indem sie eine für die Fingereingabe optimierte Benutzeroberfläche zulässt oder verweigert, die für Tablet-Geräte optimiert ist.

Standardmäßig wird eine für die Fingereingabe optimierte Benutzeroberfläche verwendet.

Setzen Sie diese Richtlinie auf "Nicht zugelassen", um nur die Windows-Benutzeroberfläche zu verwenden.

## Kombinationsfelder remoten

Diese Einstellung bestimmt die Typen von Kombinationsfeldern, die in Sitzungen auf mobilen Geräten angezeigt werden können. Stellen Sie diese Richtlinie auf Zugelassen ein, um das gerätenative Kombinationsfeld-Steuerelement anzuzeigen. Wenn diese Einstellung zugelassen ist, kann ein Benutzer eine Sitzungseinstellung in Citrix Receiver für iOS ändern und das Windows-Kombinationsfeld verwenden.

Standardmäßig wird die Funktion zum Remoten von Kombinationsfeldern verweigert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Multimedia"

Jul 08, 2016

Der Abschnitt "Multimedia" enthält Richtlinieneinstellungen, mit denen Sie das Streaming von Audio und Video in Benutzersitzungen verwalten.

## Videoqualität beschränken

Mit dieser Einstellung geben Sie die maximale Videoqualitätsstufe für eine HDX-Verbindung an. Wird die Einstellung konfiguriert, dann wird die Videoqualität auf den angegebenen Wert beschränkt, sodass die Dienstqualität für Multimedia in der Umgebung gewährleistet ist.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Zum Festlegen der maximalen Qualität wählen Sie eine der folgenden Optionen:

- 1080p/8,5 MBit/s
- 720p/4,0 MBit/s
- 480p/720 KBit/s
- 380p/400 KBit/s
- 240p/200 KBit/s

Hinweis: Die gleichzeitige Wiedergabe mehrerer Videos auf einem Server verbraucht viele Ressourcen und kann die Skalierbarkeit des Servers beeinträchtigen.

## Multimediakonferenzen

Mit dieser Einstellung legen Sie fest, ob die Unterstützung von Videokonferenzanwendungen zugelassen ist.

Standardmäßig ist die Unterstützung für Videokonferenzen zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein.

Für Multimediakonferenzen müssen folgende Bedingungen erfüllt sein:

- Der Gerätetreiber des Herstellers für die in der Multimediakonferenz verwendete Webcam muss installiert sein.
- Die Webcam muss mit dem Clientgerät verbunden werden, bevor eine Videokonferenzsitzung initiiert wird. Der Server verwendet zu jedem Zeitpunkt nur eine installierte Webcam. Wenn mehrere Webcams auf dem Benutzergerät installiert sind, versucht der Server nacheinander jede Webcam zu verwenden, bis eine Videokonferenzsitzung steht.

## Optimierung von Windows Media-Multimediaumleitung über WAN

Mit dieser Einstellung aktivieren Sie die Multimediatranscodierung in Echtzeit. Damit wird Audio- und Videostreaming für mobile Geräte ermöglicht und die Benutzererfahrung durch eine verbesserte Übermittlung von Windows Media-Inhalt über WAN optimiert.

Standardmäßig wird die Bereitstellung von Windows Media-Inhalt über das WAN optimiert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein.

Wenn diese Einstellung aktiviert ist, wird die Multimediatranscodierung nach Bedarf automatisch bereitgestellt, sodass Audio- und Videostreaming zur Verbesserung der Benutzererfahrung auch bei schlechten Netzwerkbedingungen ermöglicht


© 1999-2017 Citrix Systems, Inc. All rights reserved.

wird.

### GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden

Mit dieser Einstellung wird die Transcodierung von Multimediainhalten in Echtzeit im Grafikprozessor (GPU) des Virtual Delivery Agent (VDA) ermöglicht, um die Serverskalierbarkeit zu verbessern. Die GPU-Transcodierung ist nur verfügbar, wenn der VDA eine unterstützte GPU für die Hardwarebeschleunigung hat. Andernfalls erfolgt die Transcodierung automatisch in der CPU.

Hinweis: GPU-Transcodierung wird nur von NVIDIA-GPUs unterstützt.
Standardmäßig ist die Verwendung der GPU auf dem VDA zum Optimieren der Bereitstellung von Windows Media-Inhalt über das WAN nicht zulässig.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, stellen Sie sicher, dass die Einstellungen Windows Media-Umleitung und Optimierung von Windows Media-Multimediaumleitung über WAN vorhanden und auf Zugelassen gesetzt sind.

### Verhindern von Videofallback

Administratoren können über die Einstellung der Richtlinie "Verhindern von Videofallback" die Methoden für die Übertragung gestreamter Inhalte an Benutzer festlegen.

Standardmäßig ist diese Einstellung nicht konfiguriert. Dies ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Serverseitiger Abruf - Serverseitige Wiedergabe**: ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server.
- **Serverseitiger Abruf - Clientseitige Wiedergabe**: ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE, jedoch kein Fallback von RAVE auf den Server.
- **Clientseitiger Abruf - Clientseitige Wiedergabe**: lässt kein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server zu.

Wird der Inhalt nicht wiedergegeben, wird im Playerfenster gemeldet, dass das Video wegen mangelnder Ressourcen blockiert wurde.

### Clientseitiger Abruf von Windows Media-Inhalten

Diese Einstellung ermöglicht das Streamen von Multimediadateien anstatt über den Hostserver direkt vom Quellanbieter im Internet oder Intranet auf Benutzergeräte.

Standardmäßig ist das direkte Streaming von Multimediadateien vom Quellenanbieter auf Benutzergeräte zulässig.

Zulassen dieser Einstellung verbessert die Netzwerknutzung und Serverskalierbarkeit durch Verschieben der gesamten Medienverarbeitung vom Hostserver auf das Benutzergerät. Dadurch wird auch das Erfordernis der Installation eines erweiterten Multimedia-Frameworks, z. B. von Microsoft DirectShow oder Media Foundation, auf Benutzergeräten hinfällig. Diese müssen lediglich eine Datei von einer URL abspielen können.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein. Wenn diese Einstellung deaktiviert ist, ist das direkte Streaming von Multimediadateien auf Benutzergeräte ebenfalls deaktiviert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Windows Media-Umleitung

Diese Einstellung steuert und optimiert die Art und Weise, mit der Streamingaudio und -video Benutzern von Servern bereitgestellt wird.

Standardmäßig ist das Streamen von Audio und Video für Benutzer zulässig.

Zulassen dieser Einstellung erhöht die Qualität von auf dem Server wiedergegebenem Audio und Video auf ein Niveau, das dem der lokalen Wiedergabe auf dem Benutzergerät entspricht. Der Server streamt Multimediainhalte komprimiert im Originalformat zum Client, Dekomprimierung und Wiedergabe der Medien übernimmt das Benutzergerät.

Die Windows Media-Umleitung optimiert Multimediadateien, die mit Codecs verschlüsselt sind, die den Standards von Microsoft DirectShow, DirectX Media Objects (DMO) und Media Foundation entsprechen. Um eine Multimediadatei wiederzugeben, muss ein mit dem Codierungsformat der Multimediadatei kompatibler Codec auf dem Benutzergerät vorhanden sein.

In der Standardeinstellung ist Audio auf Citrix Receiver deaktiviert. Wenn Benutzer Multimedia-Anwendungen in ICA-Sitzungen ausführen können, aktivieren Sie Audio oder geben Sie den Benutzern in der Citrix Receiver-Benutzeroberfläche die Berechtigung, Audio zu aktivieren.

Wählen Sie Verweigert nur, wenn die Wiedergabe von Medien mit der Windows Medienumleitung schlechter zu sein scheint, als mit der ICA-Komprimierung und regulärem Audio. Dies ist selten, kann aber mit geringer Bandbreite vorkommen, beispielsweise bei Medien, in denen die Schlüsselbilder (Keyframes) sehr weit auseinander liegen.

### Windows Media-Umleitungspuffergröße

Mit dieser Einstellung geben Sie für die Multimediabeschleunigung eine Puffergröße zwischen 1 und 10 Sekunden an.

Die Standardpuffergröße ist 5 Sekunden.

### Verwendung von Windows Media-Umleitungspuffergröße

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung der unter Windows Media-Umleitungspuffergröße angegebenen Puffergröße.

In der Standardeinstellung wird die angegebene Puffergröße nicht verwendet.

Wenn diese Einstellung deaktiviert oder die Einstellung für die Windows Media-Umleitungspuffergröße nicht konfiguriert ist, verwendet der Server den Standardwert für die Puffergröße (5 Sekunden).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Multistreamverbindungen"

Jul 08, 2016

Im Abschnitt "Multistreamverbindungen" finden Sie Richtlinieneinstellungen zum Verwalten der Quality-of-Service-Priorität (QoS) für mehrere ICA-Verbindungen in einer Sitzung.

## Audio über UDP

Mit dieser Einstellung legen Sie fest, ob Audio über UDP auf dem Server zugelassen wird.

Standardmäßig ist Audio über UDP auf dem Server zugelassen.

Wenn diese Einstellung aktiviert ist, wird ein UDP-Port auf dem Server geöffnet, sodass alle Verbindungen, die zur Verwendung von Audio über UDP - Real-time Transport konfiguriert sind, unterstützt werden.

## Audio-UDP-Portbereich

Mit dieser Einstellung geben Sie den Bereich der Portnummern an (im Format niedrigste Portnummer,höchste Portnummer), die von Virtual Desktop Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet werden. Der VDA versucht, jedes UDP-Portpaar für den Austausch von Daten mit dem Benutzergerät zu verwenden. Dabei wird mit dem Port, der die niedrigste Nummer hat, begonnen und die Zahl für jeden folgenden Versuch um 2 erhöht. Alle Ports übernehmen eingehende und ausgehende Datenübertragungen.

Die Standardeinstellung ist 16500,16509.

## Multiportrichtlinie

Mit dieser Einstellung geben Sie die TCP-Ports an, die für den ICA-Verkehr verwendet werden sollen, und legen eine Netzwerkpriorität für jeden Port fest.

Standardmäßig hat der primäre Port (2598) eine hohe Priorität.

Wenn Sie Ports konfigurieren, können Sie die folgenden Prioritäten zuweisen:

- Sehr hoch: für Echtzeitvorgänge, z. B. Webkonferenzen.
- Hoch: für interaktive Elemente, z. B. Bildschirm, Tastatur und Maus.
- Mittel: für Massenvorgänge, z. B. Clientlaufwerkzuordnung.
- Niedrig: für Hintergrundaufgaben, z. B. Drucken.

Jeder Port muss eine eindeutige Priorität haben. Sie können also nicht eine sehr hohe Priorität sowohl für CGP-Port 1 als auch für CGP-Port 3 zuweisen.

Wenn Sie für einen Port keine Priorität einstellen möchten, setzen Sie den Wert für den Port auf 0. Sie können den primären Port nicht entfernen und Sie können seine Prioritätsstufe nicht ändern.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu. Diese Einstellung wird nur angewendet, wenn die Richtlinie Multistreamcomputereinstellung aktiviert ist.

## Multistreamcomputereinstellung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Server.

Standardmäßig ist Multistream deaktiviert.

Wenn Sie Citrix Cloudbridge mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu, um sicherzustellen, dass die Änderungen wirksam werden.
Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, wie beispielsweise Bandbreitenlimit für Sitzung insgesamt kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.

### Multistreambenutzereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Benutzergerät.

Standardmäßig ist Multistream für alle Benutzer deaktiviert.

Diese Einstellung wird nur auf Hosts angewendet, für die die Richtlinie Multistreamcomputereinstellung aktiviert ist.
Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, z. B. Bandbreitenlimit für Sitzung insgesamt, kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Portumleitung"

Jul 08, 2016

Der Abschnitt "Portumleitung" enthält Richtlinieneinstellungen für die LPT- und COM-Portzuordnung auf dem Client.

Verwenden Sie bei Virtual Delivery Agent-Versionen **vor 7.0** die folgenden Richtlinieneinstellungen zum Konfigurieren der Portumleitung. Konfigurieren Sie bei VDA **7.0 bis 7.8** diese Einstellungen über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung). Verwenden Sie bei VDA-Version **7.9** die folgenden Richtlinieneinstellungen.

## Client-COM-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von COM-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden COM-Ports nicht automatisch verbunden.

## Client-LPT-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von LPT-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden LPT-Ports nicht automatisch verbunden.

## Client-COM-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf COM-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die COM-Portumleitung nicht zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für COM-Portumleitung
- Bandbreitenlimit für COM-Portumleitung (Prozent)

## Client-LPT-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf LPT-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die LPT-Portumleitung nicht zugelassen.

LPT-Ports werden nur von Legacyanwendungen verwendet, die Druckaufträge an LPT-Ports senden und nicht an die Druckerobjekte auf dem Benutzergerät. Die meisten Geräte können heute Druckaufträge and Druckerobjekte senden. Diese Richtlinieneinstellung ist nur für Server erforderlich, auf denen Legacyanwendungen gehostet werden, die für das Drucken LPT-Ports verwenden.

Obwohl die COM-Portumleitung des Clients bidirektional ist, ist die LPT-Portumleitung nur für die Ausgabe und in einer ICA-Sitzung auf \\client\LPT1 und \\client\LPT2 beschränkt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für LPT-Portumleitung
- Bandbreitenlimit für LPT-Portumleitung (Prozent)


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Drucken"

Jul 08, 2016

Der Abschnitt "Drucken" enthält Richtlinieneinstellungen für die Verwaltung des Clientdrucks.

## Clientdruckerumleitung

Mit dieser Einstellung legen Sie fest, ob Clientdrucker einem Server zugeordnet werden können, wenn sich ein Benutzer an einer Sitzung anmeldet.

Standardmäßig ist die Clientdruckerzuordnung zugelassen. Wenn diese Einstellung deaktiviert ist, wird der PDF-Drucker für die Sitzung nicht automatisch erstellt.

Verwandte Richtlinieneinstellungen: Clientdrucker automatisch erstellen

## Standarddrucker

Mit dieser Einstellung geben Sie an, wie der Standarddrucker in einer ICA-Sitzung ermittelt wird.

Standardmäßig wird der aktuelle Standarddrucker auf dem Clientgerät als Standarddrucker in der Sitzung verwendet.

Mit Standarddrucker des Benutzers nicht anpassen werden die aktuellen Einstellungen für den Standarddrucker in den Remotedesktopdiensten oder im Windows-Benutzerprofil verwendet. Wenn Sie diese Option auswählen, wird der Standarddrucker nicht im Profil gespeichert und ändert sich nicht entsprechend den anderen Sitzungs- oder Clienteigenschaften. Der Standarddrucker in einer Sitzung ist der erste Drucker, der in der Sitzung automatisch erstellt wird. Das ist:

- Der erste Drucker, der lokal auf dem Windows-Server unter Systemsteuerung > Geräte und Drucker hinzugefügt wurde.
- Der erste automatisch erstellte Drucker, wenn auf dem Server keine Drucker lokal hinzugefügt wurden.

Verwenden Sie diese Option, um Benutzern über Profileinstellungen den nächstgelegenen Drucker anzubieten (Proximitydrucken).

## Druckerzuweisungen

Diese Einstellung bietet eine Alternative zu den Einstellungen Standarddrucker und Sitzungsdrucker. Mit den einzelnen Einstellungen für Standarddrucker und Sitzungsdrucker können Sie das Verhalten einer Site, einer großen Gruppe oder einer Organisationseinheit konfigurieren. Mit der Einstellung Druckerzuweisungen weisen Sie eine große Gruppe Drucker mehreren Benutzern zu.

Mit dieser Einstellung geben Sie an, wie der Standarddrucker auf den aufgeführten Benutzergeräten in einer Sitzung ermittelt wird.

Standardmäßig wird der aktuelle Standarddrucker auf dem Clientgerät als Standarddrucker in der Sitzung verwendet.

Mit dieser Einstellung geben Sie außerdem die Netzwerkdrucker an, die in einer Sitzung für jedes Benutzergerät automatisch erstellt werden sollen. In der Standardeinstellung sind keine Drucker angegeben.

- Beim Einstellen des Standarddruckerwerts:
  Wenn Sie den aktuellen Standarddrucker für das Benutzergerät verwenden möchten, wählen Sie Nicht anpassen.

  Mit Nicht anpassen werden die aktuellen Einstellungen für den Standarddrucker in den Remotedesktopdiensten oder im


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows-Benutzerprofil verwendet. Wenn Sie diese Option auswählen, wird der Standarddrucker nicht im Profil gespeichert und ändert sich nicht entsprechend den anderen Sitzungs- oder Clienteigenschaften. Der Standarddrucker in einer Sitzung ist der erste Drucker, der in der Sitzung automatisch erstellt wird. Das ist:

  - Der erste Drucker, der lokal auf dem Windows-Server unter Systemsteuerung > Geräte und Drucker hinzugefügt wurde.
  - Der erste automatisch erstellte Drucker, wenn auf dem Server keine Drucker lokal hinzugefügt wurden.
- Beim Einstellen des Sitzungsdruckerwerts: Zum Hinzufügen eines Druckers geben Sie den UNC-Pfad des Druckers ein, der automatisch erstellt werden soll. Nach dem Hinzufügen des Druckers können Sie angepasste Einstellungen für die aktuelle Sitzung bei jeder Anmeldung anwenden.

### Ereignisprotokollpräferenz für die automatische Druckererstellung

Mit dieser Einstellung geben Sie an, welche Ereignisse bei der automatischen Druckererstellung protokolliert werden. Sie haben die Option, keine Fehler oder Warnungen, nur Fehler oder Fehler und Warnungen zu protokollieren.

Standardmäßig werden Fehler und Warnungen protokolliert.

Ein Beispiel für eine Warnung ist ein Ereignis, bei dem der native Druckertreiber für einen Drucker nicht installiert werden konnte und stattdessen der universelle Druckertreiber installiert wurde. Damit der universelle Druckertreiber in diesem Szenario verwendet werden kann, stellen Sie für Verwendung universeller Druckertreiber entweder Nur universelles Drucken verwenden oder Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist ein.

### Sitzungsdrucker

Mit dieser Einstellung geben Sie die Netzwerkdrucker an, die in einer ICA-Sitzung automatisch erstellt werden sollen.

In der Standardeinstellung sind keine Drucker angegeben.

Um Drucker hinzuzufügen, geben Sie den UNC-Pfad des Druckers ein, der automatisch erstellt werden soll. Nach dem Hinzufügen des Druckers können Sie angepasste Einstellungen für die aktuelle Sitzung bei jeder Anmeldung anwenden.

### Warten bis Drucker erstellt sind (Serverdesktop)

Mit dieser Einstellung legen Sie fest, ob es eine Verzögerung bei der Sitzungsverbindung geben soll, sodass Serverdesktopdrucker automatisch erstellt werden können.

Standardmäßig findet keine Verbindungsverzögerung statt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Clientdrucker"

Jul 08, 2016

Der Abschnitt "Clientdrucker" enthält Richtlinieneinstellungen für Clientdrucker, einschließlich solcher zur automatischen Erstellung von Clientdruckern, zum Speichern von Druckereigenschaften und zum Verbinden mit Druckservern.

## Clientdrucker automatisch erstellen

Mit dieser Einstellung geben Sie die Clientdrucker an, die automatisch erstellt werden. Diese Einstellung überschreibt die Standardeinstellungen für die automatische Clientdruckererstellung.

Standardmäßig werden alle Clientdrucker automatisch erstellt.

Diese Einstellung gilt nur, wenn die Einstellung Clientdruckerumleitung vorhanden und Zugelassen ist.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Alle Clientdrucker automatisch erstellen werden alle Drucker auf dem Clientgerät erstellt.
- Mit Nur Standarddrucker des Clients automatisch erstellen wird der Drucker automatisch erstellt, der auf dem Clientgerät als Standarddrucker angegeben wurde.
- Mit Nur lokale Clientdrucker (keine Netzwerkdrucker) automatisch erstellen werden nur die Drucker automatisch erstellt, die über einen LPT-, COM-, USB-, TCP/IP- oder anderen lokalen Port direkt mit dem Clientgerät verbunden sind.
- Mit Clientdrucker nicht automatisch erstellen wird die automatische Erstellung von Clientdruckern beim Anmelden der Benutzer deaktiviert. Die Remotedesktopdienste-Einstellungen für die automatische Erstellung von Clientdruckern überschreiben dann diese Einstellung in Richtlinien mit niedrigerer Priorität.

## Generischen universellen Drucker automatisch erstellen

Hinweis: Hotfixes für Probleme aufgrund dieser Richtlinieneinstellung sind in den Knowledge Center-Artikeln CTX141565 und CTX141566 verfügbar.
Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen, in denen ein Benutzergerät verwendet wird, das mit der universellen Drucklösung kompatibel ist.

Standardmäßig wird das generische universelle Druckerobjekt nicht automatisch erstellt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Verwendung universeller Druckertreiber
- Priorität universeller Treiber

## Clientdruckernamen

Mit dieser Einstellung legen Sie die Namenskonvention für automatisch erstellte Drucker fest.

Standardmäßig werden die Standardnamen der Drucker verwendet.

Wählen Sie Standarddruckernamen, um Druckernamen im Format "HPLaserJet 4 von Clientname in Sitzung 3" zu verwenden.

Wählen Sie Legacydruckernamen, um Clientdruckernamen im alten Stil zuzulassen und die Rückwärtskompatibilität für Benutzer oder Gruppen zu erhalten, die MetaFrame Presentation Server 3.0 oder früher verwenden. Ein Beispiel für einen Legacydruckernamen ist "Client/clientname#/HPLaserJet 4". Diese Option ist weniger sicher.
Hinweis: Diese Option wird nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Direkte Verbindungen zu Druckservern

Mit dieser Einstellung aktivieren oder deaktivieren Sie direkte Verbindungen vom virtuellen Desktop oder Server, auf dem Anwendungen gehostet werden, zu einem Druckserver für Clientdrucker in einer zugänglichen Netzwerkfreigabe.

Standardmäßig sind direkte Verbindungen aktiviert.

Aktivieren Sie direkte Verbindungen, wenn der Netzwerkdruckserver für virtuelle Desktops bzw. für Server, auf denen Anwendungen gehostet werden, nicht über ein WAN zugänglich ist. Direkte Verbindungen gestatten schnelleres Drucken, wenn der Netzwerkdruckserver und der virtuelle Desktop oder Anwendungsserver sich im gleichen LAN befinden.

Deaktivieren Sie direkte Verbindungen, wenn das Netzwerk über ein WAN verläuft oder hohe Latenz oder beschränkte Bandbreite aufweist. Druckaufträge werden durch das Benutzergerät und den Netzwerkdruckserver geleitet. Daten werden komprimiert an das Benutzergerät gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

Wenn zwei Netzwerkdrucker den gleichen Namen haben, wird der Drucker benutzt, der im gleichen Netzwerk ist wie der Client.

### Druckertreiberzuordnung und -kompatibilität

Mit dieser Einstellung legen Sie Regeln für die Treiberersetzung bei automatisch erstellten Druckern fest.

In der Standardeinstellung sind keine Regeln angegeben.

Wenn Sie Regeln für die Treiberersetzung definieren, können Sie zulassen oder verhindern, dass Drucker mit dem angegebenen Treiber erstellt werden. Außerdem können Sie für erstellte Drucker nur universelle Druckertreiber zulassen. Bei der Treiberersetzung werden die Namen der Druckertreiber, die das Benutzergerät bereitstellt, überschrieben oder zugeordnet und ein äquivalenter Treiber auf dem Server wird ersetzt. So können Serveranwendungen auf Clientdrucker zuzugreifen, die denselben Treiber wie der Server, aber unterschiedliche Treibernamen verwenden.

Sie können eine Treiberzuordnung hinzufügen, eine bestehende Zuordnung bearbeiten, benutzerdefinierte Einstellungen für eine Zuordnung überschreiben oder die Reihenfolge der Treibereinträge in der Liste ändern. Um eine Zuordnung hinzuzufügen, geben Sie den Clientdruckertreibernamen an und wählen dann den Ersatztreiber auf dem Server aus.

### Speicherung von Druckereigenschaften

Mit dieser Einstellung geben Sie an, ob die Druckereigenschaften gespeichert werden und wo.

Standardmäßig ermittelt das System, ob Druckereigenschaften auf dem Clientgerät (falls verfügbar) gespeichert werden oder im Benutzerprofil.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Wählen Sie Nur auf dem Clientgerät speichern, wenn Sie ein vorgeschriebenes oder servergespeichertes Profil verwenden, das nicht gespeichert wird. Wählen Sie diese Option nur aus, wenn auf allen Servern in der Farm XenApp 5 oder höher ausgeführt wird und die Benutzer die Citrix Online Plug-In-Versionen 9 bis 12.x oder Citrix Receiver 3.x verwenden.
- Wählen Sie Nur im Benutzerprofil speichern, wenn das System durch die Bandbreite (diese Option reduziert den Datenverkehr im Netzwerk) und die Anmeldegeschwindigkeit begrenzt ist oder die Benutzer Legacy-Plug-Ins verwenden. Bei dieser Option werden die Druckereigenschaften im Benutzerprofil auf dem Server gespeichert. Die Eigenschaften werden nicht mit dem Clientgerät ausgetauscht. Verwenden Sie diese Option für MetaFrame Presentation Server 3.0 oder früher und MetaFrame Presentation Server Client 8.x oder früher. Dies gilt nur, wenn ein servergespeichertes Profil für Remotedesktopdienste (RDS) verwendet wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Mit Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind kann das System festlegen, wo die Druckereigenschaften gespeichert werden. Die Druckereigenschaften werden auf dem Clientgerät gespeichert, sofern es verfügbar ist, ansonsten im Benutzerprofil. Diese Option bietet zwar die größte Flexibilität, kann jedoch die Anmeldezeit verlangsamen und zusätzliche Bandbreite für die Systemprüfung verbrauchen.
- Druckereigenschaften nicht speichern verhindert das Speichern von Druckereigenschaften.

### Gespeicherte und wiederhergestellte Clientdrucker

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Speichern und Neuerstellen von Clientdruckern. Standardmäßig werden Clientdrucker automatisch gespeichert und automatisch wiederhergestellt.

Gespeicherte Drucker sind vom Benutzer erstellte Drucker, die beim Start der nächsten Sitzung wiederhergestellt werden. Wenn XenApp einen gespeicherten Drucker wiederhergestellt, werden alle Richtlinieneinstellungen außer Clientdrucker automatisch erstellen berücksichtigt.

Gespeicherte Drucker sind Drucker die von einem Administrator vollständig angepasst wurden und deren gespeicherter Zustand permanent mit einem Clientport verbunden ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Treiber"

Jul 08, 2016

Der Abschnitt "Treiber" enthält Richtlinieneinstellungen für Druckertreiber.

## Automatische Installation von mitgelieferten Druckertreibern

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Installation von Druckertreibern vom standardmäßigen Windows-Treibersatz oder von Treiberpaketen, die auf dem Host mit pnputil.exe /a bereitgestellt wurden.

Standardmäßig werden diese Treiber bei Bedarf installiert.

## Priorität universeller Treiber

Mit dieser Einstellung geben Sie an, in welcher Reihenfolge die universellen Druckertreiber verwendet werden, angefangen mit dem ersten Eintrag in der Liste.

Standardmäßig ist die Prioritätsreihenfolge wie folgt:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Sie können Treiber hinzufügen, bearbeiten oder entfernen und die Reihenfolge der Treiber in der Liste ändern.

## Verwendung universeller Druckertreiber

Mit dieser Einstellung geben Sie an, wann universelles Drucken verwendet wird.

Standardmäßig wird universelles Drucken nur verwendet, wenn der angeforderte Treiber nicht verfügbar ist.

Universelles Drucken verwendet allgemeine Druckertreiber statt modellspezifischer Standardtreiber; dies verringert potentiell den Aufwand für die Treiberverwaltung auf Hostcomputern. Die Verfügbarkeit universeller Druckertreiber hängt von den Funktionen des Benutzergeräts, des Hosts und der Druckserversoftware ab. In bestimmten Konfigurationen steht universelles Drucken möglicherweise nicht zur Verfügung.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Nur druckermodellspezifische Treiber verwenden verwendet der Clientdrucker nur die modellspezifischen Standardtreiber, die bei der Anmeldung automatisch erstellt wurden. Wenn der erforderliche Treiber nicht verfügbar ist, kann der Clientdrucker nicht automatisch erstellt werden.
- Nur universelles Drucken verwenden gibt an, dass keine modellspezifischen Standardtreiber verwendet werden. Nur universelle Druckertreiber werden zum Erstellen von Druckern verwendet.
- Mit Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist werden modellspezifische Standardtreiber für die Druckererstellung verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden universellen Treiber erstellt.
- Mit Druckermodellspezifische Treiber nur verwenden, wenn universelles Drucken nicht verfügbar ist werden universelle Druckertreiber verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden modellspezifischen Druckertreiber erstellt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Universeller Druckserver"

Jul 08, 2016

Der Abschnitt "Universeller Druckserver" enthält Richtlinieneinstellungen für die Behandlung des universellen Druckservers.

## Universellen Druckserver aktivieren

Diese Einstellung aktiviert oder deaktiviert das Feature "Universeller Druckserver" auf dem virtuellen Desktop oder dem Server, auf dem Anwendungen gehostet werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

Standardmäßig ist das Feature deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der folgenden Optionen:

- **Aktiviert mit Fallback auf systemeigenen Windows-Remotedruck**: Netzwerkdruckerverbindungen werden nach Möglichkeit vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, wird der Windows-Druckanbieter verwendet. Der Windows-Druckanbieter handhabt weiterhin alle Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden.
- **Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck**: Netzwerkdruckerverbindungen werden ausschließlich vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, schlägt die Netzwerkdruckerverbindung fehl. Mit dieser Einstellung wird der Netzwerkdruck über den Windows-Druckanbieter effektiv deaktiviert. Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden, werden nicht erstellt, solange eine Richtlinie mit dieser Einstellung aktiv ist.
- **Deaktiviert**: Das Feature "Universeller Druckserver" ist deaktiviert. Beim Herstellen einer Verbindung mit einem Netzwerkdrucker, der einen UNC-Namen hat, wird keine Verbindung mit dem universellen Druckserver versucht. Verbindungen mit Remotedruckern verwenden weiterhin den Windows-Remotedruck.

## Port für Druckdatenstrom des universellen Druckservers (CGP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet wird. Wenden Sie diese Richtlinie nur für Organisationseinheiten an, die den Druckserver enthalten.

Die Standardeinstellung der Portnummer ist "7229".

Gültige Portnummern müssen im Bereich von 1 bis 65535 liegen.

## Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)

Diese Einstellung gibt das obere Limit (in Kilobit pro Sekunde) für die Übertragungsrate der Druckdaten an, die von jedem Druckauftrag mit CGP an den universellen Druckserver übergeben werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

In der Standardeinstellung ist der Wert 0, was angibt, dass es kein oberes Limit gibt.

## Port für universellen Druckserverwebdienst (HTTP/SOAP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom HTTP/SOAP-Webdienstlistener des universellen Druckservers verwendet wird. Der universelle Druckserver ist eine optionale Komponente, mit der die Verwendung universeller Druckertreiber von Citrix für den Netzwerkdruck ermöglicht wird. Wird der universelle Druckserver verwendet, werden die Druckbefehle von den XenApp- und XenDesktop-Hosts mit SOAP über HTTP an den universellen Druckserver gesendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Durch diese Einstellung ändert sich die Nummer des Standard-TCP-Ports, der vom Webdienstlistener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen überwacht wird.

Sie müssen den gleichen HTTP- Port für Host und Druckserver konfigurieren. Wenn Sie nicht den gleichen Port konfigurieren, stellt die Hostsoftware keine Verbindung mit dem universellen Druckserver her. Durch diese Einstellung ändert sich der VDA unter XenApp und XenDesktop. Außerdem müssen Sie den Standardport auf dem Computer mit dem universellen Druckserver ändern.

Die Standardeinstellung der Portnummer ist "8080".

Gültige Portnummern müssen im Bereich von 0 bis 65535 liegen.

### Universelle Druckserver für den Lastausgleich

Mit dieser Einstellung werden die universellen Druckserver aufgelistet, die zum Lastausgleich für am Sitzungsstart erstellte Druckerverbindungen verwendet werden, nachdem andere Citrix Druckrichtlinieneinstellungen bewertet wurden. Zum Optimieren der Erstellungszeit von Druckern empfiehlt Citrix, dass alle Druckserver über denselben Satz freigegebener Drucker verfügen. Es gibt kein Maximum für die Anzahl von Druckservern, die für den Lastausgleich hinzugefügt werden können.

Diese Einstellung implementiert auch Druckserver-Failovererkennung und die Wiederherstellung von Druckerverbindungen. Die Druckserver werden regelmäßig auf Verfügbarkeit überprüft. Wenn ein Serverfehler erkannt wird, wird der Server aus dem Lastausgleichsschema entfernt und Druckerverbindungen auf dem Server werden auf andere verfügbare Druckserver verteilt. Wenn der fehlerhafte Druckserver wiederhergestellt ist, wird er dem Lastausgleichsschema wieder hinzugefügt.

Klicken Sie auf **Server überprüfen**, um zu prüfen, ob die einzelnen Server Druckserver sind, und um sicherzustellen, dass auf allen Druckservern ein identischer Satz freigegebener Drucker installiert ist. Dieser Vorgang kann einige Zeit dauern.

### Außer-Betrieb-Schwellenwert für universelle Druckserver

Mit dieser Einstellung wird angegeben, wie lange der Load Balancer auf die Wiederherstellung eines nicht verfügbaren universellen Druckservers wartet, bevor der Server als offline gilt und die Last des Servers auf andere verfügbare Druckserver verteilt wird.

Der Standardschwellenwert ist 180 (Sekunden).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Universelles Drucken"

Jul 08, 2016

Der Abschnitt "Universelles Drucken"" enthält Richtlinieneinstellungen für die Verwaltung des universellen Drucks.

## Universelles Drucken - EMF-Verarbeitungsmodus

Mit dieser Einstellung steuern Sie die Verarbeitungsmethode für die EMF-Spooldatei auf dem Windows-Benutzergerät.

Standardmäßig werden EMF-Datensätze direkt zum Drucker gespoolt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- EMF-Datensätze für Drucker neu verarbeiten erzwingt die Neuverarbeitung der EMF-Spooldatei und sendet sie durch das GDI-Teilsystem auf dem Benutzergerät. Sie können diese Einstellung für Treiber verwenden, für die eine EMF-Neuverarbeitung erforderlich ist, die jedoch nicht unbedingt in der Sitzung automatisch ausgewählt werden.
- Wenn Direkt zum Drucker spoolen mit dem universellen Citrix Druckertreiber verwendet wird, werden die EMF-Datensätze garantiert gespoolt und an das Benutzergerät für die Verarbeitung übergeben. Diese EMF-Spooldateien werden normalerweise direkt in die Spoolwarteschlange des Clients gesetzt. Für Drucker und Treiber, die mit dem EMF-Format kompatibel sind, ist dies die schnellste Druckmethode.

## Universelles Drucken - Bildkomprimierungslimit

Mit dieser Einstellung geben Sie die maximale Qualität und minimale Komprimierung für Bilder an, die mit dem universellen Citrix Druckertreiber gedruckt werden.

Das Limit für Bildkomprimierung ist standardmäßig auf Beste Qualität (verlustfreie Komprimierung) gesetzt.

Wenn Keine Komprimierung ausgewählt ist, wird die Komprimierung nur für den EMF-Druck deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Keine Komprimierung
- Beste Qualität (verlustfreie Komprimierung)
- Hohe Qualität
- Standardqualität
- Geringere Qualität (maximale Komprimierung)

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards" enthält, achten Sie auf Folgendes:

- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Bildkomprimierungslimit komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

## Universelles Drucken - Optimierungsstandards

Mit dieser Einstellung geben Sie die Standardwerte für die Druckoptimierung an, wenn der universelle Druckertreiber für eine Sitzung erstellt wurde.

- Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
- Mit Heavyweight-Komprimierung aktivieren aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von Gewünschte Bildqualität festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
- Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert. Hinweis: Diese Einstellungen gelten nur, wenn das Benutzergerät dieses Verhalten unterstützt.
- Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht ändern.

Hinweis: Alle diese Optionen werden für den EMF-Druck unterstützt. Für XPS-Druck wird nur die Option Gewünschte Bildqualität unterstützt.
Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards" enthält, achten Sie auf Folgendes:
- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Bildkomprimierungslimit komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

### Universelles Drucken - Vorschaueinstellung

Mit dieser Einstellung geben Sie an, ob die Druckvorschau für automatisch erstellte oder universelle Drucker verwendet werden soll.

Standardmäßig wird die Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwendet.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:
- Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden
- Druckervorschau nur für automatisch erstellte Drucker verwenden
- Druckvorschau nur für generische universelle Drucker verwenden
- Druckvorschau für automatisch erstellte und generische universelle Drucker verwenden

### Universelles Drucken - Druckqualitätslimit

Diese Einstellung legt den Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung fest.

Standardmäßig ist Kein Limit aktiviert, d. h. Benutzer können die höchste Druckqualität auswählen, die vom Drucker zugelassen wird, mit dem sie eine Verbindung herstellen.

Wenn diese Einstellung konfiguriert ist, wird die maximale Druckqualität, die Benutzern zur Verfügung steht, hinsichtlich Ausgabeauflösung beschränkt. Sowohl die Druckqualität und die Druckqualitätsmerkmale des Druckers, mit dem sich die Benutzer verbinden, werden auf die konfigurierte Einstellung beschränkt. Beispiel: Wenn Mittlere Auflösung (600 dpi) konfiguriert ist, können Benutzer eine Ausgabe nur mit einer maximalen Qualität von 600 drucken, und die Einstellung "Druckqualität" auf der Registerkarte "Erweitert" im Dialogfeld "Universeller Drucker" enthält nur Auflösungseinstellungen bis zu "Mittlere Qualität (600 dpi).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Entwurf (150 dpi)
- Niedrige Auflösung (300 dpi)
- Mittlere Auflösung (600 dpi)
- Hohe Auflösung (1200 dpi)
- Kein Limit


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Sicherheit"

Jul 08, 2016

Der Abschnitt "Sicherheit" enthält die Richtlinieneinstellung zum Konfigurieren der Sitzungsverschlüsselung und der Anmeldedatenverschlüsselung.

## SecureICA-Mindestverschlüsselungsgrad

Mit dieser Einstellung geben Sie das Minimum für den Verschlüsselungsgrad der Sitzungsdaten an, die zwischen dem Server und einem Clientgerät ausgetauscht werden.

**Wichtig:** Bei Virtual Delivery Agent 7.x kann mit dieser Richtlinieneinstellung nur die Anmeldedatenverschlüsselung mit RC5 128-Bit-Verschlüsselung aktiviert werden. Die anderen Einstellungen werden nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.

Bei VDA 7.x wird die Sitzungsdatenverschlüsselung mit den Grundeinstellungen der Bereitstellungsgruppe des VDAs festgelegt. Wenn für die Bereitstellungsgruppe die Option "Secure ICA aktivieren" ausgewählt ist, werden Sitzungsdaten mit der RC5-Verschlüsselung (128 Bit) verschlüsselt. Wenn die Option "Secure ICA aktivieren" für die Bereitstellungsgruppe nicht ausgewählt ist, werden Sitzungsdaten mit der Basic-Verschlüsselung verschlüsselt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Basic verschlüsselt die Clientverbindung mit einem nicht RC5-konformen Algorithmus. Mit diesem Verschlüsselungsverfahren kann der Datenstrom zwar vor direktem Lesen geschützt werden, ein Entschlüsseln ist aber möglich. Standardmäßig verwendet der Server für den Client-Server-Netzwerkverkehr den Verschlüsselungsgrad "Basic".
- RC5 (128 Bit) nur Anmeldung verschlüsselt die Anmeldedaten mit der RC5-128-Bit-Verschlüsselung und die Clientverbindung mit dem Verschlüsselungsgrad "Basic".
- RC5 (40 Bit) verschlüsselt die Verbindung mit der RC5-40-Bit-Verschlüsselung.
- RC5 (56 Bit) verschlüsselt die Verbindung mit der RC5-56-Bit-Verschlüsselung.
- RC5 (128 Bit) verschlüsselt die Verbindung mit der RC5-128-Bit-Verschlüsselung.

Die Einstellungen, die Sie für die Verschlüsselung zwischen Client und Server festlegen, können mit Verschlüsselungseinstellungen des Windows-Betriebssystems interagieren. Wenn ein höherer Verschlüsselungsgrad auf dem Server oder Benutzergerät eingestellt ist, können Einstellungen überschrieben werden, die Sie für veröffentlichte Ressourcen angegeben haben.

Sie können den Verschlüsselungsgrad erhöhen, um die Kommunikation und Datenintegrität für bestimmte Benutzer stärker zu sichern. Wenn für eine Richtlinie ein höherer Verschlüsselungsgrad erforderlich ist, wird Citrix Receivern mit einem niedrigeren Verschlüsselungsgrad die Verbindung verweigert.

SecureICA führt keine Authentifizierung durch und prüft auch nicht die Datenintegrität. Verwenden Sie SecureICA mit TLS-Verschlüsselung, um eine vollständige Verschlüsselung für die Site bereitzustellen.

SecureICA verwendet nicht FIPS-konforme Algorithmen. Wenn dies ein Problem ist, konfigurieren Sie den Server und Citrix Receiver, um zu verhindern, dass SecureICA verwendet wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Serverlimits"

Jul 08, 2016

Der Abschnitt "Serverlimits" enthält die Richtlinieneinstellung zum Steuern von Sitzungen im Leerlauf.

## Serverleerlauf-Zeitintervall

Mit dieser Einstellung geben Sie in Millisekunden an, wie lange eine ununterbrochene Benutzersitzung erhalten bleibt, wenn keine Benutzereingaben stattfinden.

Standardmäßig werden Leerlaufsitzungen nicht getrennt (Serverleerlaufzeitintervall = 0)

> ### Hinweis
>
> Bei Verwendung dieser Richtlinie wird Benutzern u. U. ein Dialogfeld mit der Meldung "Leerlauf-Timer abgelaufen" angezeigt, wenn die Sitzung die angegebene Zeit lang im Leerlauf war. Dies ist ein MicrosoftDialogfeld, das nicht von Citrix Richtlinieneinstellungen gesteuert wird. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX118618.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Sitzungslimits"

Jul 08, 2016

Der Abschnitt "Sitzungslimits" enthält Richtlinieneinstellungen, mit denen Sie die Dauer der Sitzungen festlegen können, bevor diese getrennt werden.

## Timer für getrennte Sitzung

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, der angibt, wie lange ein getrennter, gesperrter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird.

Standardmäßig werden getrennte Sitzungen nicht abgemeldet.

## Getrennte Sitzungen - Timerintervall

Mit dieser Einstellung legen Sie fest, wie viele Minuten ein getrennter, gesperrter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird.

Standardmäßig sind es 1440 Minuten (24 Stunden).

## Sitzungsverbindungstimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, mit dem die maximale Dauer einer ununterbrochenen Sitzung zwischen einem Benutzergerät und einem Desktop festgelegt wird.

Standardmäßig ist dieser Timer aktiviert.

## Sitzungsverbindung - Timerintervall

Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop in Minuten fest.

Standardmäßig ist die maximale Dauer 1440 Minuten (24 Stunden).

## Sitzungsleerlauftimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, der angibt, wie lange eine ununterbrochene Benutzergeräteverbindung mit einem Desktop erhalten bleibt, wenn keine Benutzereingaben stattfinden.

Standardmäßig ist dieser Timer deaktiviert.

## Sitzungsleerlauf - Timerintervall

Diese Einstellung legt fest, wie viele Minuten eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem Desktop aufrechterhalten wird, wenn keine Eingabe vom Benutzer erfolgt.

Standardmäßig bleiben Leerlaufsitzungen 1440 Minuten (24 Stunden) erhalten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Sitzungszuverlässigkeit"

Jul 08, 2016

Der Abschnitt "Sitzungszuverlässigkeit" enthält Richtlinieneinstellungen zum Verwalten von Verbindungen, für die die Sitzungszuverlässigkeit verwendet wird.

## Sitzungszuverlässigkeit - Verbindungen

Mit dieser Einstellung legen Sie fest, ob Sitzungen bei dem Verlust der Netzwerkkonnektivität offen bleiben sollen.

Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Wenn die Netzwerkverbindung unterbrochen ist, friert der Bildschirm auf dem Client ein und der Mauszeiger wird als Sanduhr angezeigt, bis die Verbindung wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder. Wenn Sie möchten, dass Benutzer eine Verbindung zu unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können, stellen Sie Authentifizierung bei automatischer Wiederverbindung von Clients entsprechend ein. Benutzer werden dann aufgefordert, sich neu zu authentifizieren, wenn sie sich mit der unterbrochenen Sitzung wiederverbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option Sitzungszuverlässigkeit - Timeout festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

## Sitzungszuverlässigkeit - Portnummer

Mit dieser Einstellung geben Sie die TCP-Portnummer für eingehende Sitzungszuverlässigkeitsverbindungen an.

Die Standardeinstellung der Portnummer ist "2598".

## Sitzungszuverlässigkeit - Timeout

Mit dieser Einstellung legen Sie fest, wie viele Sekunden der Sitzungszuverlässigkeitsproxy auf die Wiederverbindung der Sitzung wartet, bevor die Sitzung getrennt wird.

Die Standardeinstellung ist 180 Sekunden (3 Minuten).

Sie können zwar eine Sitzung länger offen lassen, beachten Sie jedoch, dass Benutzer nicht zu einer Neuauthentifizierung aufgefordert werden, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Zeitzonensteuerung"

Jul 08, 2016

Der Abschnitt "Zeitzonensteuerung" enthält Richtlinieneinstellungen für die Zeitzone in Sitzungen.

## Lokale Zeitzone für Legacyclients schätzen

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Schätzen der lokalen Zeitzone auf Clientgeräten, die falsche Zeitzoneninformationen an den Server senden.

Standardmäßig schätzt der Server die lokale Zeitzone, wenn erforderlich.

Diese Einstellung ist für die Verwendung mit älteren Citrix Receiver-Versionen oder ICA- Clients vorgesehen, die keine detaillierten Zeitzoneninformationen an den Server senden. Bei Verwendung mit Citrix Receiver-Versionen, die detaillierte Zeitzoneninformationen an den Server senden, beispielsweise die unterstützten Versionen von Citrix Receiver für Windows, hat diese Einstellung keine Auswirkung.

## Lokale Zeit des Clients verwenden

Mit dieser Einstellung legen Sie die Zeitzoneneinstellung der Benutzersitzung fest. Dies kann entweder die Zeitzone der Sitzung des Benutzers oder die des Benutzergeräts sein.

Standardmäßig wird die Zeitzone der Sitzung des Benutzers verwendet.

Damit diese Einstellung wirksam wird, aktivieren Sie die Einstellung Zeitzonenumleitung zulassen im Gruppenrichtlinien-Editor (Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung > Geräte- und Ressourcenumleitung).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "TWAIN-Geräte"

Jul 08, 2016

Der Abschnitt "TWAIN-Geräte" enthält Richtlinieneinstellungen für die Zuordnung von TWAIN-Geräten, wie Digitalkameras oder Scanner, und für das Optimieren der Bildübertragung vom Server zum Client.

> **Hinweis**
>
> TWAIN 2.0 wird zurzeit nicht unterstützt.

## TWAIN-Geräteumleitung für Client

Mit dieser Einstellung legen Sie fest, ob Benutzer auf TWAIN-Geräte auf dem Benutzergerät aus Bildverarbeitungsanwendungen auf Servern zugreifen können. Standardmäßig ist die TWAIN-Geräteumleitung zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- TWAIN-Komprimierungsgrad
- Bandbreitenlimit für TWAIN-Geräteumleitung
- Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

## TWAIN-Komprimierungsgrad

Mit dieser Einstellung geben Sie den Komprimierungsgrad für Bildübertragungen vom Client zum Server an. Verwenden Sie Gering für die beste Bildqualität, Mittel für eine gute Bilderqualität und Hoch für eine geringe Bildqualität. Standardmäßig wird die mittlere Komprimierung angewendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "USB-Geräte"

Jul 08, 2016

Der Abschnitt "USB-Geräte" enthält Richtlinieneinstellungen für die Verwaltung der Dateiumleitung bei USB-Geräten.

## Regeln für die Client-USB-Geräteoptimierung

Regeln für die Client-USB-Geräteoptimierung können auf Geräte angewendet werden, um die Optimierung zu deaktivieren oder den Optimierungsmodus zu ändern.

Wenn ein Benutzer ein USB-Gerät anschließt, prüft der Host, ob das Gerät gemäß den USB-Richtlinieneinstellungen zulässig ist. Ist das Gerät zulässig, prüft der Host die **Regeln für die Client-USB-Geräteoptimierung** für das Gerät. Wenn keine Regel angegeben ist, wird das Gerät im interaktiven Modus behandelt (02). Aufnahmemodus (04) ist der empfohlene Modus für Signaturgeräte. Eine Beschreibung der Modi finden Sie unten.

**Gut zu wissen**

- Für die Verwendung von Wacom Signatur-Tablets empfiehlt Citrix, dass Sie den Bildschirmschoner deaktivieren. Anweisungen hierzu finden Sie am Ende dieses Abschnitts.
- Unterstützung für die Optimierung von Wacom-Signatur-Tablets der STU-Reihe ist in der Installation von Richtlinien bei XenApp und XenDesktop vorkonfiguriert.
- Signaturgeräte funktionieren lückenlos in XenApp und XenDesktop und erfordern zur Verwendung als Signaturgerät keine Treiber. Wacom bietet zusätzliche Software an, die zur weiteren Anpassung des Geräts installiert werden kann. Informationen finden Sie unter http://www.wacom.com/.
- Grafiktablets: Bestimmte Grafik-Eingabegeräte werden als HID-Gerät an einem PCI/ACPI-Bus präsentiert und nicht unterstützt. Diese Geräte müssen an einen USB-Hostcontroller auf dem Client angeschlossen werden, damit sie innerhalb der XenDesktop-Sitzung umgeleitet werden.

Richtlinienregeln haben das Format von durch Leerzeichen getrennten Tag=Wert-Ausdrücken. Die folgenden Tags werden unterstützt:

| Tagname | Beschreibung |
|---|---|
| Modus | Der Optimierungsmodus wird für Eingabegeräte der Klasse 3 (class=**03**) unterstützt. Unterstützte Modi:<br><br>Keine Optimierung: Wert **01**.<br><br>Interaktiver Modus: Wert **02**. Empfohlen für Geräte wie Stift-Tablets und 3D Pro-Mäuse.<br><br>Erfassungsmodus: Wert **04**. Vorzugsmodus für Signatur-Tablets und ähnliche Geräte. |
| VID | Hersteller-ID vom Gerätedeskriptor |
| PID | Produkt-ID vom Gerätedeskriptor |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| REL | Release-ID vom Gerätedeskriptor |
| Klasse | Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor |
| SubClass | Unterklasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor |
| Prot | Protokoll vom Gerätedeskriptor oder einem Schnittstellendeskriptor |

**Beispiele**

Mode=00000004 VID=1230 PID=1230 class=03 (Eingabegerät im Erfassungsmodus)

Mode=00000002 VID=1230 PID=1230 class=03 (Eingabegerät im interaktiven Modus, Standardeinstellung)

Mode=00000001 VID=1230 PID=1230 class=03 (Eingabegerät ohne Optimierung)

Mode=00000100 VID=1230 PID=1230 (Setupoptimierung deaktiviert, Standardeinstellung)

Mode=00000200 VID=1230 PID=1230 (Setupoptimierung aktiviert)

**Deaktivieren des Optimierungsmodus mittels einer Einstellung in der Registrierung**

Der Optimierungsmodus kann systemweit über folgendes Registrierungskennzeichen deaktiviert werden:

HKLM\System\CurrentControlSet\Services\Icausbb\Parameters

**DisableInputOptimization** DWORD – Wert auf **1** festlegen

Es ist ein Systemneustart erforderlich, damit diese Änderung wirksam wird.

**Deaktivieren des Bildschirmschoners für Wacom-Signatur-Tablets**

Für die Verwendung von Wacom Signatur-Tablets sollten Sie den Bildschirmschoner wie folgt deaktivieren:

1. Installieren Sie den Wacom-STU-Treiber nach der Umleitung des Geräts.
2. Installieren Sie das **Wacom-STU-Display-MSI**, um Zugriff auf die Systemsteuerung des Signatur-Tablets zu erhalten.
3. Navigieren Sie zu **Control Panel > Wacom STU Display > STU430** oder **STU530** und wählen Sie die Registerkarte für das jeweilige Modell aus.
4. Klicken Sie auf **Change** und wählen Sie **Yes**, wenn das Fenster für die UAC-Sicherheit angezeigt wird.
5. Wählen Sie **Disable slideshow** und klicken Sie auf **Apply**.

Wenn die Einstellung für ein Signatur-Tabletmodell festgelegt ist, wird sie auf alle Modelle angewendet.

## Client-USB-Geräteumleitung

Mit dieser Einstellung legen Sie fest, ob die Umleitung von USB-Geräten zu und von Benutzergeräten zulässig ist.

Standardmäßig werden USB-Geräte nicht umgeleitet.

## Regeln für die Client-USB-Geräteumleitung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung legen Sie die Umleitungsregeln für USB-Geräte fest.

In der Standardeinstellung sind keine Regeln angegeben.

Schließt ein Benutzer ein USB-Gerät an, prüft das Hostgerät jede Richtlinienregel, bis eine Übereinstimmung vorliegt. Die erste Übereinstimmung für ein beliebiges Gerät ist entscheidend. Ist es eine Zulassen-Regel, kann das Gerät remote auf dem virtuellen Desktop verwendet werden. Ist es eine Verweigern-Regel, kann das Gerät nur auf dem lokalen Desktop verwendet werden. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.

Richtlinienregeln haben das Format {Allow:|Deny:} plus Tag=Wert, durch Leerzeichen getrennt. Die folgenden Tags werden unterstützt:

| Tagname | Beschreibung |
|---|---|
| VID | Vendor-ID vom Gerätedeskriptor |
| PID | Produkt-ID vom Gerätedeskriptor |
| REL | Release-ID vom Gerätedeskriptor |
| Klasse | Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor |
| SubClass | Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor |
| Prot | Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor |

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird.
- Leere Zeilen und Kommentare werden ignoriert.
- Tags müssen den Übereinstimmungsoperator = verwenden, z. B. VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.
- USB-Klassencodes finden Sie auf der Website von USB Implementers Forum, Inc.

Beispiel für administratordefinierte USB-Richtlinienregeln:

- Allow: VID=1230 PID=0007 # Weitere Industrie, Weiteres Flash-Laufwerk
- Deny: Class=08 SubClass=05 # Massenspeichergeräte
- Eine Regel, die alle USB-Geräte verweigert, erstellen Sie mit "DENY:" ohne weitere Tags.

### Client-USB-Geräteumleitung für Plug & Play-Geräte

Mit dieser Einstellung legen Sie fest, ob Plug & Play-Geräte, wie Kameras oder POS-Geräte (Point of Sale) in einer Clientsitzung verwendet werden können.

In der Standardeinstellung ist die Umleitung von Plug & Play-Geräten zugelassen. Bei der Einstellung Zugelassen werden alle Plug & Play-Geräte für einen bestimmten Benutzer oder eine bestimmte Benutzergruppe umgeleitet. Bei der Einstellung Nicht zugelassen werden keine Geräte umgeleitet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Visuelle Anzeige"

Jul 08, 2016

Der Abschnitt "Visuelle Anzeige" enthält Richtlinieneinstellungen, mit denen die Qualität der von virtuellen Desktops an das Benutzergerät gesendeten Bilder gesteuert wird.

## Bevorzugte Farbtiefe für einfache Grafiken

Ermöglicht die Verringerung der Farbtiefe für das Senden einfacher Grafiken auf **16 Bit pro Pixel**, was potenziell unter geringen Einbußen bei der Bildqualität die Reaktion bei Verbindungen mit geringer Bandbreite verbessert. Diese Option wird nur unterstützt, wenn kein Videocodec zum Komprimieren von Grafiken verwendet wird.

Die Standardeinstellung ist 24 Bit pro Pixel.

## Frameratesollwert

Mit dieser Einstellung geben Sie die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden.

In der Standardeinstellung ist die Höchstanzahl 30 Frames pro Sekunde.

Die Festlegung auf eine hohe Anzahl von Frames pro Sekunde (z. B. 30) führt zu einer besseren Benutzererfahrung, erfordert aber mehr Bandbreite. Wenn Sie die Anzahl von Frames pro Sekunde herabsetzen (z. B. auf 10), wird die Serverskalierbarkeit auf Kosten der Benutzererfahrung erhöht. Bei Benutzergeräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung.

## Bildqualität

Mit dieser Einstellung legen Sie die Bildqualität für auf dem Benutzergerät angezeigte Bilder fest.

Die Standardeinstellung ist "Mittel".

Zum Festlegen der Bildqualität wählen Sie eine der folgenden Optionen:

- **Niedrig**
- **Mittel**: bietet die beste Leistung und Bandbreiteneffizienz in den meisten Anwendungsfällen.
- **Hoch**: empfiehlt sich, wenn visuell verlustfreie Bildqualität gewünscht wird.
- **Zu verlustfrei verbessern**: sendet verlustreiche Bilder in Zeiträumen mit hoher Netzwerkaktivität und verlustfreie Bilder bei verringerter Netzwerkaktivität an das Benutzergerät. Mit dieser Einstellung wird die Leistung bei Netzwerkverbindungen mit beschränkter Bandbreite verbessert.
- **Immer verlustfrei**: In Situationen, in denen kein Qualitätsverlust akzeptabel ist (z. B. bei der Anzeige von Röntgenbildern), wählen Sie Immer verlustfrei, um sicherzustellen, dass keine verlustreichen Daten an das Benutzergerät gesendet werden.

Wenn die Einstellung **Legacygrafikmodus** aktiviert ist, hat die Einstellung **Bildqualität** keine Auswirkungen in der Richtlinie.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Bewegtbilder"

Aug 17, 2016

Der Abschnitt "Bewegtbilder" enthält Einstellungen, mit denen Sie die Komprimierung für dynamische Bilder entfernen oder ändern können.

> ## Hinweis
>
> Bei VDAs der Version 7.0 bis 7.6 gelten die Richtlinieneinstellungen für **Bewegtbildkomprimierung** und **Mindestframeratesollwert** nur, wenn **Legacygrafikmodus** aktiviert ist. Bei VDAs ab Version 7.6 FP1 und höher gelten diese Einstellungen unabhängig davon, ob der Legacygrafikmodus deaktiviert oder aktiviert ist.

### Bewegtbildkomprimierung

Mit dieser Einstellung wird angegeben, ob der adaptive Bildschirm aktiviert ist. Der adaptive Bildschirm passt die Bildqualität von Videos und Bildübergängen in Diashows auf der Grundlage der verfügbaren Bandbreite automatisch an. Bei aktiviertem adaptivem Bildschirm werden Benutzern gleichmäßig ausgeführte Präsentationen ohne Qualitätseinbußen angezeigt. Standardmäßig ist der adaptive Bildschirm aktiviert.

Bei VDAs der Version 7.0 bis 7.6 gilt diese Einstellung nur, wenn der Legacygrafikmodus aktiviert ist. Bei VDAs ab Version 7.6 FP1 gilt diese Einstellung, wenn der Legacygrafikmodus aktiviert ist oder wenn der Legacygrafikmodus deaktiviert ist und kein Videocodec zum Komprimieren von Grafiken verwendet wird.

Wenn der Legacygrafikmodus aktiviert ist, muss die Sitzung neu gestartet werden, damit die Richtlinienänderungen wirksam werden. Adaptive Anzeige und progressive Anzeige schließen einander aus, d. h. durch Aktivieren der adaptiven Anzeige wird die progressive Anzeige deaktiviert und umgekehrt. Allerdings können progressive und adaptive Anzeige zur gleichen Zeit deaktiviert sein. Die progressive Anzeige wird als Legacyfeature für XenApp und XenDesktop nicht empfohlen. Durch Festlegen des Schwellenwerts für die progressive Komprimierung wird die adaptive Anzeige deaktiviert.

### Mindestframeratesollwert

Mit dieser Einstellung wird die Framerate pro Sekunde eingestellt, die das System für dynamische Bilder in Netzwerken mit geringer Bandbreite versucht beizubehalten.
Die Standardeinstellung für diesen Parameter ist 10 F/s.

> ## Hinweis
>
> Bei Virtual Delivery Agent 7.x gelten die folgenden Richtlinieneinstellungen nur, wenn die Richtlinieneinstellung **Legacygrafikmodus** aktiviert ist.

### Mindestbildqualität

Mit dieser Einstellung wird die zulässige Mindestbildqualität für den adaptiven Bildschirm angegeben. Je geringer die verwendete Komprimierung ist, desto höher ist die Qualität der angezeigten Bilder. Es stehen folgende Komprimierungen zur Verfügung: Ultrahoch, Sehr hoch, Hoch, Normal und Niedrig.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Standardeinstellung ist "Normal".

### Grad der progressiven Komprimierung

Mit dieser Einstellung wird zuerst ein weniger detailliertes Bild angezeigt, das dafür aber schneller dargestellt werden kann. In der Standardeinstellung wird keine progressive Komprimierung angewendet.

Sobald es verfügbar ist, wird ein detailreicheres Bild anzeigt, das die normale Einstellung für verlustreiche Komprimierung verwendet. Verwenden Sie sehr hohe oder ultrahohe Komprimierung für die verbesserte Anzeige von bandbreitenintensiven Grafiken, wie etwa Fotografien.

Die progressive Komprimierung ist nur wirksam, wenn der Komprimierungsgrad höher ist als die Einstellung für Grad der verlustreichen Komprimierung.
Hinweis: Der stärkere Komprimierungsgrad für die progressive Komprimierung verbessert auch die Interaktivität von dynamischen Bildern über Clientverbindungen. Die Qualität eines dynamischen Bilds, z. B. ein sich drehendes dreidimensionales Modell, wird temporär verringert, bis das Bild stehen bleibt. Zu dem Zeitpunkt wird dann die reguläre Einstellung der verlustreichen Komprimierung angewendet.
Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung

### Schwellenwert für progressive Komprimierung

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die progressive Komprimierung angewendet wird. Die Komprimierung wird nur für Clientverbindungen unter diesem Bandbreitenwert verwendet.
Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Standbilder"

Aug 17, 2016

Der Abschnitt "Standbilder" enthält Einstellungen, mit denen Sie die Komprimierung für statische Bilder entfernen oder ändern können.

> **Hinweis**
>
> Bei Virtual Delivery Agent 7.x gelten diese Richtlinieneinstellungen nur, wenn die Richtlinieneinstellung **Legacygrafikmodus** aktiviert ist.

## Zusätzliche Farbkomprimierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung der zusätzlichen Farbkomprimierung für Bilder, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden; dies verbessert die Reaktionszeit, da die Bilder in geringerer Qualität angezeigt werden.
Standardmäßig ist die zusätzliche Farbkomprimierung deaktiviert.

Bei Aktivierung wird die zusätzliche Farbkomprimierung nur angewendet, wenn die Bandbreite der Clientverbindung unter dem für Schwellenwert für zusätzliche Farbkomprimierung festgelegten Wert liegt. Wenn die Bandbreite der Clientverbindung über dem Schwellenwert liegt oder Deaktiviert ausgewählt ist, wird die zusätzliche Farbkomprimierung nicht angewendet.

## Schwellenwert für zusätzliche Farbkomprimierung

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, unter der die zusätzliche Farbkomprimierung angewendet wird. Wenn die Bandbreite der Clientverbindung unter den eingestellten Wert abfällt, wird die zusätzliche Farbkomprimierung (falls aktiviert) angewendet.
Der Standardschwellenwert ist 8192 Kilobits pro Sekunde.

## Heavyweight-Komprimierung

Mit dieser Einstellung reduzieren Sie die erforderliche Bandbreite noch stärker als mit der progressiven Komprimierung, ohne dabei an Bildqualität zu verlieren, indem ein verbesserter grafischer Algorithmus verwendet wird, der aber mehr CPU beansprucht.
Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.

Wenn die Heavyweight-Komprimierung aktiviert ist, gilt sie für alle verlustreichen Komprimierungen. Diese Einstellung wird von Citrix Receiver unterstützt, hat aber keine Auswirkung auf andere Plug-Ins.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Grad der progressiven Komprimierung
- Schwellenwert für progressive Komprimierung

## Grad der verlustreichen Komprimierung

Mit dieser Einstellung steuern Sie den Grad der verlustreichen Komprimierung, der für Grafiken verwendet wird, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden. In solchen Fällen kann die Anzeige von Bildern ohne


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Komprimierung sehr langsam sein.
Standardmäßig wird eine mittlere Komprimierung ausgewählt.

Bessere Reaktionszeiten bei bandbreitenintensiven Bildern erzielen Sie mit hoher Komprimierung. In Fällen, in denen die Bilddaten erhalten bleiben müssen, beispielsweise bei der Anzeige von Röntgenbildern, wo kein Qualitätsverlust akzeptabel ist, sollten Sie die verlustreiche Komprimierung nicht einsetzen.

Verwandte Richtlinieneinstellung: Schwellenwert für verlustreiche Komprimierung

### Schwellenwert für verlustreiche Komprimierung

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die die verlustreiche Komprimierung angewendet wird.
Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Wenn Sie die Einstellung Grad der verlustreichen Komprimierung einer Richtlinie hinzufügen, ohne einen Schwellenwert anzugeben, kann sich dadurch die Anzeigegeschwindigkeit für detailreiche Bitmaps, wie Fotografien, über ein LAN verbessern.

Verwandte Richtlinieneinstellung: Grad der verlustreichen Komprimierung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "WebSockets"

Jul 08, 2016

Der Abschnitt "WebSockets" enthält Richtlinieneinstellungen für den Zugriff auf virtuelle Desktops und gehostete Anwendungen mit Citrix Receiver für HTML5. Das Feature WebSockets erhöht die Sicherheit und verringert die Last durch bidirektionale Kommunikation zwischen browserbasierten Anwendungen und Servern ohne Öffnen von mehreren HTTP-Verbindungen.

## WebSockets-Verbindungen

Diese Einstellung lässt WebSockets-Verbindungen zu oder lehnt sie ab.

Standardmäßig sind WebSocket-Verbindungen nicht zulässig.

## WebSockets-Portnummer

Mit dieser Einstellung wird der Port für eingehende WebSocket-Verbindungen festgelegt.

In der Standardeinstellung ist der Wert 8008.

## Vertrauenswürdige WebSockets-Ursprungsserverliste

Diese Einstellung bietet eine durch Trennzeichen getrennte Liste der vertrauenswürdigen Ursprungsserver, normalerweise Citrix Receiver für Web, in Form von URLs. Nur WebSockets-Verbindungen, die von einer dieser Adressen stammen, werden vom Server akzeptiert.

Standardmäßig wird der Platzhalter * verwendet. Damit wird allen Citrix Receiver für Web-URLs vertraut.

Wenn Sie eine Adresse in die Liste eingeben möchten, verwenden Sie folgende Syntax:

<Protokoll>://<Vollqualifizierter Domänenname des Hosts>:[Port]

Das Protokoll muss HTTP oder HTTPS sein. Wenn der Port nicht angegeben wird, wird Port 80 für HTTP und Port 443 für HTTPS verwendet.

Der Platzhalter * kann innerhalb der URL verwendet werden, außer als Teil einer IP-Adresse (10.105. *. *).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Lastverwaltung"

Jul 08, 2016

Der Abschnitt "Lastverwaltung" enthält Richtlinieneinstellungen für das Aktivieren und Konfigurieren des Lastausgleichs zwischen Servern, über die Windows Server-Betriebssystemmaschinen bereitgestellt werden.

Weitere Informationen zum Berechnen des Lastauswertungsindex finden Sie unter CTX202150.

## Toleranzwert für gleichzeitige Anmeldungen

Mit dieser Einstellung geben Sie die maximal zulässige Anzahl gleichzeitiger Anmeldungen bei einem Server an.

Die Standardeinstellung ist 2.

## CPU-Nutzung

Mit dieser Einstellung geben Sie den Prozentsatz der CPU-Nutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die CPU-Nutzung wird bei der Lastberechnung nicht berücksichtigt.

## CPU-Nutzung ausschließlich Prozesspriorität

Mit dieser Einstellung geben Sie die Prioritätsstufe an, bei der die Prozess-CPU-Auslastung vom Lastindex der CPU-Nutzung ausgeschlossen wird.

Die Standardeinstellung ist "Unter normal oder niedrig".

## Datenträgernutzung

Mit dieser Einstellung geben Sie die Länge der Datenträgerwarteschlange an, zu der der Server 75 % Volllast meldet. Der Standardwert dieser Einstellung ist 8.

Standardmäßig ist diese Einstellung deaktiviert und die Datenträgernutzung wird bei der Lastberechnung nicht berücksichtigt.

## Sitzungshöchstanzahl

Mit dieser Einstellung geben Sie die maximale Anzahl von Sitzungen an, die von einem Server gehostet werden können. Ist die Einstellung aktiviert, beträgt der Standardwert für die maximale Anzahl Sitzungen an, die von einem Server gehostet werden können, 250.

Standardmäßig ist diese Einstellung aktiviert.

## Speichernutzung

Mit dieser Einstellung geben Sie den Prozentsatz der Speichernutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die Speichernutzung wird bei der Lastberechnung nicht berücksichtigt.

## Speichernutzung - Ausgangslast


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung geben Sie einen Näherungswert der Speichernutzung durch das Basisbetriebssystem in MB an, unterhalb dessen die Speichernutzung bei einem Server als Nulllast interpretiert wird.

Der Standardwert dieser Einstellung ist 768 MB.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Profilverwaltung"

Jul 08, 2016

Der Abschnitt "Profilverwaltung" enthält Richtlinieneinstellungen zum Aktivieren der Profilverwaltung und zum Konfigurieren der Gruppen, die in die Verarbeitung der Profilverwaltung eingeschlossen bzw. ausgeschlossen werden sollen.

Weitere Informationen, wie die Namen der entsprechenden INI-Dateieinstellungen und die für eine Richtlinieneinstellung erforderliche Version der Profilverwaltung, finden Sie unter Profilverwaltungsrichtlinien.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Erweitert"

Jul 08, 2016

Der Abschnitt "Erweitert" enthält Richtlinieneinstellungen für die erweiterte Konfiguration der Profilverwaltung.

## Automatische Konfiguration deaktivieren

Mit dieser Einstellung legen Sie fest, dass die Umgebung von der Profilverwaltung untersucht werden kann, z. B., um zu überprüfen, ob persönliche vDisks vorhanden sind, und um die Gruppenrichtlinie entsprechend zu konfigurieren. Nur Richtlinien für die Profilverwaltung mit dem Status "Nicht konfiguriert" werden angepasst, sodass alle zuvor vorgenommenen Anpassungen beibehalten werden. Dieses Feature beschleunigt die Bereitstellung und vereinfacht die Optimierung. Es ist keine Konfiguration des Features ist erforderlich aber Sie können die automatische Konfiguration bei Upgrades (zum Beibehalten der Einstellungen von früheren Versionen) oder bei der Problembehandlung deaktivieren. Die automatische Konfiguration funktioniert in XenApp oder anderen Umgebungen nicht.

In der Standardeinstellung ist die automatische Konfiguration zugelassen.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die automatische Konfiguration aktiviert. Einstellungen der Profilverwaltung können sich dann möglicherweise ändern, wenn sich die Umgebung ändert.

## Benutzer bei Problem abmelden

Mit dieser Einstellung wird eine Abmeldung eines Benutzers durch die Profilverwaltung ermöglicht, wenn ein Problem auftritt, z. B. wenn der Benutzerspeicher nicht verfügbar ist. Wenn diese Einstellung aktiviert ist, wird dem Benutzer eine Fehlermeldung angezeigt, bevor er abgemeldet wird. Wenn diese Einstellung deaktiviert ist, erhalten Benutzer ein temporäres Profil.

Standardmäßig ist diese Einstellung deaktiviert und Benutzer erhalten ein temporäres Profil, wenn ein Problem auftritt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird ein temporäres Profil bereitgestellt.

## Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien

Mit dieser Einstellung geben Sie die Anzahl der Zugriffsversuche auf gesperrte Dateien durch die Profilverwaltung an.

Der Standardwert dieser Einstellung ist fünf Versuche.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

## Internet-Cookiedateien bei Abmeldung verarbeiten

Mit dieser Einstellung legen Sie fest, dass die Datei index.dat beim Abmelden von der Profilverwaltung verarbeitet werden kann, damit Internet-Cookies im Dateisystem nach längerem Browsen entfernt werden. Auf diese Weise wird eine Aufblähung von Profilen vermieden. Eine Aktivierung der Einstellung verlängert die Abmeldezeiten. Aktivieren Sie sie daher nur, wenn das entsprechende Problem bei Ihnen auftritt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung verarbeitet die Datei index.dat beim Abmelden nicht.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird Index.dat nicht verarbeitet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Grundlegende Richtlinieneinstellungen

Jul 08, 2016

Der Abschnitt "Grundlegend" enthält Richtlinieneinstellungen für die grundlegende Konfiguration der Profilverwaltung.

## Aktiv zurückschreiben

Mit dieser Einstellung können geänderte Dateien und Ordner (aber keine Registrierungseinträge) während einer Sitzung mit dem Benutzerspeicher synchronisiert werden bevor die Abmeldung erfolgt.

Standardmäßig ist die Synchronisierung mit dem Benutzerspeicher während laufender Sitzungen deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie aktiviert.

## Profilverwaltung aktivieren

Mit dieser Einstellung wird die Profilverwaltung zur Verarbeitung von An- und Abmeldungen aktiviert.

Standardmäßig ist diese Einstellung deaktiviert, um die Bereitstellung zu vereinfachen.

Wichtig: Citrix empfiehlt, eine Aktivierung der Profilverwaltung erst dann durchzuführen, wenn alle anderen Setupaufgaben ausgeführt wurden und getestet wurde, wie sich Citrix Benutzerprofile in der Umgebung verhalten.
Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, verarbeitet die Profilverwaltung keine Windows-Benutzerprofile.

## Ausgeschlossene Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) nicht von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung keine Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME>\<GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.

## Unterstützung von Offlineprofilen

Mit dieser Einstellung wird die Unterstützung von Offlineprofilen aktiviert, durch die Profile nach einer Unterbrechung der Verbindung mit dem Netzwerk zum frühestmöglichen Zeitpunkt mit dem Benutzerspeicher synchronisiert werden.

Standardmäßig ist die Unterstützung von Offlineprofilen deaktiviert.

Diese Einstellung gilt für Benutzer von Laptops und mobile Benutzer im Roamingmodus. Wenn die Verbindung zum


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Netzwerk unterbrochen wird, bleiben die Profile auf dem Laptop oder Gerät intakt, selbst wenn das Gerät neu gestartet wird oder im Ruhezustand gewesen ist. Während mobile Benutzer arbeiten, werden ihre Profile lokal aktualisiert und am Ende mit dem Benutzerspeicher synchronisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist die Unterstützung von Offlineprofilen deaktiviert.

### Pfad zum Benutzerspeicher

Mit dieser Einstellung geben Sie den Pfad zu dem Verzeichnis (Benutzerspeicher) an, in dem Benutzereinstellungen, z. B. Registrierungseinstellungen und synchronisierte Dateien, gespeichert werden.

Standardmäßig wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Wenn diese Einstellung deaktiviert ist, werden die Benutzereinstellungen im Windows-Unterverzeichnis des Basisverzeichnisses gespeichert.

Mögliche Pfade:

- **Relativer Pfad**: Dieser Pfad muss relativ zum Basisverzeichnis sein. Dieses ist normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert.
- **Absoluter UNC-Pfad**: Hiermit wird üblicherweise eine Serverfreigabe oder ein DFS-Namespace angegeben.
- **Deaktiviert oder nicht konfiguriert**: In diesem Fall wird als Wert #homeDirectory#\Windows angenommen.

Verwenden Sie die folgenden Variablentypen beim Konfigurieren dieser Richtlinieneinstellung:

- Systemumgebungsvariablen in Prozentzeichen (z. B. %ProfVer%). Beachten Sie, dass Systemumgebungsvariablen normalerweise weitere Einrichtung erfordern.
- Attribute des Active Directory-Benutzerobjekts in Rauten (z. B. #sAMAccountName#).
- Profilverwaltungsvariablen. Weitere Informationen finden Sie in der Dokumentation zur Profilverwaltung.

Sie können auch mit den Benutzerumgebungsvariablen %username% und %userdomain% benutzerdefinierte Attribute erstellen, um Organisationsvariablen wie Standort und Benutzer vollständig zu definieren. Bei Attributen muss Groß- und Kleinschreibung beachtet werden.

Beispiele:

- \\Server\Freigabe\#sAMAccountName# speichert die Benutzereinstellungen unter dem UNC-Pfad \\Server\Freigabe\KurtMeier (wenn #sAMAccountName# zu Kurt Meier als aktuellem Benutzer aufgelöst wird).
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! kann erweitert werden zu \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Wichtig: Unabhängig davon, welche Attribute oder Variablen Sie verwenden, müssen Sie sicherstellen, dass diese Einstellung zu einem Ordner über dem Ordner, der NTUSER.DAT enthält, aufgelöst wird. Wenn sich diese Datei z. B. in \\Server\profiles$\KurtMeier.BuHa\v2x64\UPM_Profile befindet, geben Sie den Pfad zum Benutzerspeicher als \\Server\profiles$\KurtMeier.BuHa\v2x64 an (ohne den Unterordner \UPM_Profile) an.
Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

### Anmeldungen lokaler Administratoren verarbeiten

Mit dieser Einstellung wird angegeben, ob Anmeldungen von Mitgliedern der Gruppe "BUILTIN\Administrators" verarbeitet


© 1999-2017 Citrix Systems, Inc. All rights reserved.

werden. Dies ermöglicht es Domänenbenutzern mit lokalen Administratorrechten, d. h. normalerweise Benutzer mit zugewiesenen virtuellen Desktops, die Verarbeitung zu umgehen, sich anzumelden und Probleme mit der Profilverwaltung bei einem Desktop zu behandeln.

Wenn diese Einstellung unter Serverbetriebssystemen deaktiviert oder nicht konfiguriert ist, nimmt die Profilverwaltung an, dass Anmeldungen von Domänenbenutzern, aber nicht von lokalen Administratoren, verarbeitet werden müssen. Unter Desktopbetriebssystemen werden Anmeldungen lokaler Administratoren verarbeitet.

Diese Einstellung ist standardmäßig deaktiviert und Anmeldungen lokaler Administratoren werden nicht verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Anmeldungen lokaler Administratoren nicht verarbeitet.

### Verarbeitete Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung nur Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME>\<GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Plattformübergreifende Richtlinieneinstellungen

Jul 08, 2016

Der Abschnitt "Plattformübergreifende Einstellungen" enthält Richtlinieneinstellungen für die Konfiguration der plattformübergreifenden Einstellungen der Profilverwaltung.

## Benutzergruppen für plattformübergreifende Einstellungen

Mit dieser Einstellung geben Sie die Benutzergruppen an, deren Profile verarbeitet werden sollen, wenn das Feature für plattformübergreifende Einstellungen aktiviert ist.

Standardmäßig ist diese Einstellung deaktiviert und alle Benutzergruppen in der Richtlinieneinstellung Verarbeitete Gruppen werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

## Plattformübergreifende Einstellungen aktivieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Feature "Plattformübergreifende Einstellungen". Dieses ermöglicht das Migrieren und Roamen von Benutzerprofilen, wenn ein Benutzer eine Verbindung mit einer Anwendung herstellt, die unter mehreren Betriebssystemen ausgeführt wird.

Standardmäßig ist das Feature "Plattformübergreifende Einstellungen" deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

## Pfad zu plattformübergreifenden Definitionen

Mit dieser Einstellung geben Sie in Form eines UNC-Pfads den Netzwerkspeicherort an, der die aus dem Downloadpaket kopierten Definitionsdateien enthält.

Hinweis: Benutzer benötigen Lesezugriff und Administratoren Schreibzugriff auf diesen Speicherort, bei dem es sich entweder um eine Server Message Block-Dateifreigabe (SMB) oder eine Common Internet File System-Dateifreigabe (CIFS) handeln muss.
In der Standardeinstellung ist kein Pfad angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

## Pfad zum Speicher für plattformübergreifende Einstellungen

Diese Einstellung gibt den Pfad zum Speicher für plattformübergreifende Einstellungen an. Hier werden die plattformübergreifenden Einstellungen der Benutzer gespeichert. Der Pfad kann ein UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Benutzer müssen über Schreibzugriff auf den Speicher für plattformübergreifende Einstellungen verfügen. Standardmäßig ist diese Einstellung deaktiviert und der Pfad "Windows\PM_CP" wird verwendet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

### Quelle für plattformübergreifende Einstellungen

Mit dieser Einstellung legen Sie eine Plattform als Basisplattform fest, wenn die entsprechende Einstellung für die Organisationseinheit der Plattform aktiviert ist. Daten von den Profilen der Basisplattform werden in den Speicher für plattformübergreifende Einstellungen migriert.

Die Profile jeder Plattform werden in einer separaten Organisationseinheit gespeichert. Dies bedeutet, dass Sie die Plattform auswählen müssen, deren Profildaten zum Füllen des Speichers für plattformübergreifende Einstellungen verwendet werden sollen. Dies wird als Basisplattform bezeichnet.

Wenn diese Option aktiviert ist, migriert die Profilverwaltung die Daten des Einzelplattformprofils in den Speicher, wenn der Speicher für plattformübergreifende Einstellungen eine Definitionsdatei ohne Daten enthält oder die zwischengespeicherten Daten eines Einzelplattformprofils neuer sind als die Definitionsdaten im Speicher.

Wichtig: Wenn diese Einstellung in mehreren Organisationseinheiten für mehrere Benutzer oder Maschinenobjekte aktiviert ist, wird die Plattform, bei der sich der erste Benutzer anmeldet, zum Basisprofil.
Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung migriert die Daten des Einzelplattformprofils nicht in den Speicher.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Dateisystem"

Jul 08, 2016

Der Abschnitt "Dateisystem" enthält Richtlinieneinstellungen zum Angeben der Dateien und Verzeichnisse in einem Benutzerprofil, die zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden sollen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Ausschlüsse"

Jul 08, 2016

Der Abschnitt "Ausschlüsse" enthält Richtlinieneinstellungen zum Konfigurieren der Dateien und Verzeichnisse in einem Benutzerprofil, die von der Synchronisierung ausgeschlossen werden sollen.

## Ausschlussliste - Verzeichnisse

Mit dieser Einstellung geben Sie eine Liste der Ordner im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Geben Sie die Ordnernamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an.

Standardmäßig ist diese Einstellung deaktiviert und alle Ordner in Benutzerprofilen werden synchronisiert.

Beispiel: Desktop ignoriert den Ordner "Desktop" im Benutzerprofil.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Ordner im Benutzerprofil synchronisiert.

## Ausschlussliste - Dateien

Mit dieser Einstellung geben Sie eine Liste der Dateien im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden synchronisiert.

Geben Sie die Dateinamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an. Hinweis: Platzhalter sind zulässig und werden rekursiv angewendet.

Beispiel: "Desktop\Desktop.ini" ignoriert die Datei Desktop.ini im Verzeichnis "Desktop".

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Dateien im Benutzerprofil synchronisiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Synchronisierung"

Jul 08, 2016

Der Abschnitt "Synchronisierung" enthält Richtlinieneinstellungen für die Angabe, welche Dateien und Ordner in einem Benutzerprofil zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden.

## Zu synchronisierende Verzeichnisse

Diese Einstellung gibt die Dateien an, die sich in ausgeschlossenen Ordnern befinden und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Unterordner des Benutzerprofils einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein.

Beispiel: "Desktop\ausschließen\aufnehmen" stellt sicher, dass der Unterordner "aufnehmen" synchronisiert wird, selbst wenn das Verzeichnis "Desktop\ausschließen" nicht synchronisiert wird.

Standardmäßig ist diese Einstellung deaktiviert und keine Ordner sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Ordner im Benutzerprofil synchronisiert.

## Zu synchronisierende Dateien

Diese Einstellung gibt die Dateien an, die sich in ausgeschlossenen Ordnern befinden und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Dateien in dem Benutzerprofil einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. Relative Pfade werden als relativ zum Benutzerprofil interpretiert. Platzhalter können nur für Dateinamen verwendet werden. Platzhalter können nicht verschachtelt werden und werden rekursiv angewendet.

Beispiele:

- Anwendungsdaten\Lokal\Microsoft\Office\Access.qat gibt eine Datei unter einem Ordner an, der in der Standardkonfiguration ausgeschlossen wurde.
- Anwendungsdaten\Lokal\Anwendungen*.cfg gibt alle Dateien mit der Erweiterung .cfg im Profilordner Anwendungsdaten\Lokal\Anwendungen und dessen Unterordnern an.

Standardmäßig ist diese Einstellung deaktiviert und keine Dateien sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Dateien im Benutzerprofil synchronisiert.

## Zu spiegelnde Ordner


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung geben Sie an, welche Ordner relativ zum Stammordner eines Benutzerprofils gespiegelt werden sollen. Diese Richtlinie kann beim Lösen von Problemen bei Transaktionsordnern (auch "Referenzordner" genannt) helfen. Dies sind Ordner, die voneinander abhängige Dateien enthalten, wobei eine Datei Verweise auf andere Dateien enthält.

Durch das Spiegeln von Ordnern kann die Profilverwaltung einen Transaktionsordner und seinen Inhalt als eine Entität verarbeiten. So wird das Aufblähen von Profilen verhindert. Beachten Sie, dass in solchen Situationen der "letzte Schreibvorgang Priorität hat", d. h. dass Dateien in gespiegelten Ordnern, die in mehr als einer Sitzung geändert wurden, von der letzten Aktualisierung überschrieben werden. Hierdurch gehen Profiländerungen verloren.

Sie können z. B. den Cookies-Ordner von Internet Explorer spiegeln, damit Index.dat mit den Cookies synchronisiert wird, auf die die Datei verweist.

Wenn ein Benutzer zwei Internet Explorer-Sitzungen auf unterschiedlichen Servern hat und er in jeder Sitzung auf andere Websites zugreift, werden Cookies dieser Sites auf dem entsprechenden Server hinzugefügt. Wenn sich der Benutzer von der ersten Sitzung abmeldet (oder auch mitten in der Sitzung, wenn das Feature für aktives Zurückschreiben konfiguriert ist), sollten die Cookies der zweiten Sitzung die Cookies der ersten Sitzung ersetzen. Stattdessen werden sie jedoch zusammengeführt und die Verweise auf die Cookies in Index.dat sind infolgedessen veraltet. Weiteres Browsen in neuen Sitzungen kann zum wiederholten Zusammenführen und einem aufgeblähten Cookie-Ordner führen.

Durch Spiegeln des Cookie-Ordners wird dieses Problem gelöst, indem Cookies, jedes Mal wenn der Benutzer sich abmeldet, mit denen der letzten Sitzung überschrieben werden. So bleibt Index.dat aktuell.

Standardmäßig ist diese Einstellung deaktiviert und es werden keine Ordner gespiegelt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, werden keine Ordner gespiegelt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Ordnerumleitung"

Jul 08, 2016

Der Abschnitt "Ordnerumleitung" enthält Richtlinieneinstellungen für die Angabe, ob häufig in Profilen erscheinende Ordner an einen freigegebenen Speicherort im Netzwerk umgeleitet werden sollen.

## Administratorzugriff gewähren

Diese Einstellung ermöglicht einem Administrator den Zugriff auf den Inhalt von umgeleiteten Ordnern der Benutzer.

Diese Einstellung ist standardmäßig deaktiviert und es haben ausschließlich Benutzer Zugriff auf den Inhalt ihrer umgeleiteten Ordner.

## Domänennamen einschließen

Diese Einstellung ermöglicht die Verwendung der Umgebungsvariablen %userdomain% als Teil des für umgeleitete Ordner angegebenen UNC-Pfads.

Standardmäßig ist diese Einstellung deaktiviert und die Umgebungsvariable %userdomain% ist nicht Teil der UNC-Pfad-Angabe für umgeleitete Ordner.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "AppData(Roaming)"

Jul 08, 2016

Der Abschnitt "AppData(Roaming)" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "AppData(Roaming)" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## AppData(Roaming)-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "AppData(Roaming)" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für AppData(Roaming)

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "AppData(Roaming)" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Kontakte"

Jul 08, 2016

Der Abschnitt "Kontakte" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Kontakte" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Kontakte'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "Kontakte" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Kontakte'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Kontakte" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Desktop"

Jul 08, 2016

Der Abschnitt "Desktop" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Desktop" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Desktop'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "Desktop" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Desktop'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Desktop" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Dokumente"

Jul 08, 2016

Der Abschnitt "Dokumente" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Dokumente" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Dokumente'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner "Dokumente" umgeleitet werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Die Einstellung 'Dokumente'-Pfad muss aktiviert sein, damit Dateien sowohl in den Ordner "Dokumente" als auch in die Ordner "Bilder", "Musik" und "Videos" umgeleitet werden.

## Umleitungseinstellungen für 'Dokumente'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Dokumente" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Dokumente" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: leitet den Inhalt zu dem in der Richtlinieneinstellung 'Dokumente'-Pfad angegebenen UNC-Pfad.
- Zum Basisverzeichnis des Benutzers umleiten: leitet den Inhalt zu dem Basisverzeichnis des Benutzers. Dieses ist normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Downloads"

Jul 08, 2016

Der Abschnitt "Downloads" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Downloads" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Downloads'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner "Downloads" umgeleitet werden.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Downloads'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Downloads" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Favoriten"

Jul 08, 2016

Der Abschnitt "Favoriten" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Favoriten" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Favoriten'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Favoriten" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Favoriten'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Favoriten" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Links"

Jul 08, 2016

Der Abschnitt "Links" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Links" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Links'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Links" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Links'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Links" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Musik"

Jul 08, 2016

Der Abschnitt "Musik" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Musik" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Musik'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Musik" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Musik'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Musik" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Musik" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Musik'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner 'Dokumente' umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner "Dokumente" um.

Damit Inhalte in einen Ordner relativ zum Ordner "Dokumente" umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Bilder"

Jul 08, 2016

Der Abschnitt "Bilder" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Bilder" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## 'Bilder'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Bilder" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Umleitungseinstellungen für 'Bilder'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Bilder" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Bilder" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Bilder'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner 'Dokumente' umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner "Dokumente" um.

Damit Inhalte in einen Ordner relativ zum Ordner "Dokumente" umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Gespeicherte Spiele"

Jul 08, 2016

Der Abschnitt "Gespeicherte Spiele" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Gespeicherte Spiele" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## Umleitungseinstellungen für 'Gespeicherte Spiele'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Gespeicherte Spiele" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## 'Gespeicherte Spiele'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Gespeicherte Spiele" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Suchen"

Jul 08, 2016

Der Abschnitt "Suchen" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Suchen" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## Umleitungseinstellungen für 'Suchen'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Suchen" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## 'Suchen'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Suchen" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Startmenü"

Jul 08, 2016

Der Abschnitt "Startmenü" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Startmenü" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## Umleitungseinstellungen für 'Startmenü'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Startmenü" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Startmenü-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Startmenü" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Videos"

Jul 08, 2016

Der Abschnitt "Videos" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Videos" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

## Umleitungseinstellungen für 'Videos'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Videos" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Videos" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Videos'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner 'Dokumente' umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner "Dokumente" um.

Damit Inhalte in einen Ordner relativ zum Ordner "Dokumente" umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## 'Videos'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Videos" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Protokollierung"

Jul 08, 2016

Der Abschnitt "Protokollierung" enthält Richtlinieneinstellungen zum Konfigurieren der Protokollierung der Profilverwaltung.

## Active Directory-Aktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in Active Directory ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

## Allgemeine Informationen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Informationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

## Allgemeine Warnungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Warnungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

## Protokollierung aktivieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Protokollierung der Profilverwaltung im Debugmodus (ausführliche Protokollierung). Im Debugmodus werden umfangreiche Statusinformationen in den Protokolldateien unter "%SystemRoot%\System32\Logfiles\UserProfileManager" aufgezeichnet.

Standardmäßig ist diese Einstellung deaktiviert und es werden nur Fehler protokolliert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix empfiehlt, dass Sie diese Einstellung nur aktivieren, wenn Sie eine Problembehandlung für die Profilverwaltung durchführen.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur Fehler protokolliert.

### Dateisystemaktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der im Dateisystem ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Dateisystembenachrichtigungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Dateisystembenachrichtigungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzerabmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Anmeldebildschirm

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzeranmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Max. Größe der Protokolldatei

Mit dieser Einstellung geben Sie die maximal zulässige Größe für die Protokolldatei der Profilverwaltung in Bytes an.

Der Standardwert dieser Einstellung ist 1048576 Bytes (1 MB).

Citrix empfiehlt, dass die Größe dieser Datei auf 5 MB oder mehr erhöht wird, sofern Sie ausreichend Speicherplatz auf dem Datenträger haben. Wenn die Protokolldatei die maximale Größe überschreitet, wird eine vorhandene Sicherungskopie der Datei (.bak) gelöscht, die Protokolldatei erhält die Erweiterung .bak und eine neue Protokolldatei wird erstellt.

Die Protokolldatei wird unter "%SystemRoot%\System32\Logfiles\UserProfileManager" erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

### Pfad zur Protokolldatei

Mit dieser Einstellung geben Sie einen alternativen Pfad an, der zum Speichern der Protokolldatei der Profilverwaltung verwendet wird.

Standardmäßig ist diese Einstellung deaktiviert und Protokolldateien werden im Standardspeicherort %SystemRoot%\System32\Logfiles\UserProfileManager gespeichert.

Der Pfad kann zu einem lokalen Laufwerk oder einem Remotelaufwerk im Netzwerk (UNC-Pfad) führen. Remotepfade können in großen, verteilten Umgebungen von Nutzen sein, können aber zu erheblichem Netzwerkverkehr führen, was für Protokolldateien unangebracht ist. Geben Sie für bereitgestellte virtuelle Maschinen mit einer beständigen Festplatte einen lokalen Pfad zu diesem Laufwerk an. Hierdurch wird sichergestellt, dass Protokolldateien beim Neustart der Maschine beibehalten werden. Geben Sie für virtuelle Maschinen ohne eine beständige Festplatte einen UNC-Pfad an. So werden Protokolldateien beibehalten. Das Systemkonto für die Maschinen muss aber Schreibzugriff auf die UNC-Freigabe haben. Verwenden Sie für Laptops, die vom Feature für Offlineprofile verwaltet werden, einen lokalen Pfad.

Wenn für Protokolldateien ein UNC-Pfad verwendet wird, empfiehlt Citrix, entsprechende Zugriffssteuerungslisten auf den Ordner mit den Protokolldateien anzuwenden, um sicherzustellen, dass nur autorisierte Benutzer- oder Computerkonten auf die gespeicherten Dateien zugreifen können.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardspeicherort "%SystemRoot%\System32\Logfiles\UserProfileManager" verwendet.

### Persönliche Benutzerinformationen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung persönlicher Benutzerinformationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Richtlinienwerte bei Anmeldung und Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung der Richtlinienwerte beim An- und Abmelden von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Registrierungsaktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in der Registrierung ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

### Registrierungsunterschiede bei der Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung aller Registrierungsunterschiede bei der Abmeldung von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Profilverarbeitung"

Jul 08, 2016

Der Abschnitt "Profilverarbeitung" enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

## Verzögerung vor dem Löschen von zwischengespeicherten Profilen

Mit dieser Einstellung geben Sie optional eine Verlängerung für die Verzögerung (in Minuten) ein, nach der die Profilverwaltung lokal zwischengespeicherte Profile bei der Abmeldung löscht.

Bei einem Wert von 0 werden die Profile am Ende der Abmeldung sofort gelöscht. Die Profilverwaltung prüft jede Minute auf Abmeldungen, sodass ein Wert von 60 sicherstellt, dass Profile zwischen einer und zwei Minuten (je nachdem, wann die letzte Überprüfung stattgefunden hat) nach dem Abmelden gelöscht werden. Das Erweitern der Verzögerung ist nützlich, wenn Sie wissen, dass ein Prozess Dateien oder die Registrierungsstruktur während der Abmeldung geöffnet hält. Bei großen Profilen kann dies auch den Abmeldungsvorgang beschleunigen.

Die Standardeinstellung ist 0, lokal zwischengespeicherte Profile werden von der Profilverwaltung sofort gelöscht.

Wenn Sie diese Einstellung aktivieren, müssen Sie sicherstellen, dass die Einstellung Lokal zwischengespeicherte Profile nach Abmeldung löschen auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden die Profile sofort gelöscht.

## Lokal zwischengespeicherte Profile nach Abmeldung löschen

Mit dieser Einstellung geben Sie an, ob lokal zwischengespeicherte Profile gelöscht werden, nachdem Benutzer sich abmelden.

Wenn diese Einstellung aktiviert ist, wird der lokale Profilcache der Benutzer nach der Abmeldung gelöscht. Citrix empfiehlt, dass Sie diese Einstellung für Terminalserver aktivieren.

Standardmäßig ist diese Einstellung deaktiviert und der lokale Profilcache von Benutzern wird nach der Abmeldung beibehalten.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden zwischengespeicherte Profile nicht gelöscht.

## Behandlung von Konflikten lokaler Profile

Mit dieser Einstellung wird konfiguriert, wie die Profilverwaltung verfährt, wenn ein Benutzerprofil sowohl im Benutzerspeicher als auch als lokales Windows-Benutzerprofil (kein Citrix Benutzerprofil) vorhanden ist.

Standardmäßig verwendet die Profilverwaltung lokale Windows-Profile, ohne diese jedoch zu ändern.

Zum Steuern, wie die Profilverwaltung verfahren soll, wählen Sie eine der folgenden Optionen:

- Lokales Profil verwenden: Die Profilverwaltung verwendet lokale Windows-Profile, ohne diese jedoch zu ändern.
- Lokales Profil löschen: Die Profilverwaltung löscht das lokale Windows-Benutzerprofil und importiert dann das Citrix


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Benutzerprofil aus dem Benutzerspeicher.
- Lokales Profil umbenennen: Die Profilverwaltung benennt das lokale Windows-Benutzerprofil um (als Sicherungskopie) und importiert dann das Citrix Benutzerprofil aus dem Benutzerspeicher.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale Profile verwendet.

### Migration vorhandener Profile

Mit dieser Einstellung geben Sie den Typ des Profils an, das bei der Anmeldung eines Benutzers in den Benutzerspeicher migriert wird, wenn der Speicher kein aktuelles Profil für den Benutzer enthält.

Die Profilverwaltung kann vorhandene Profile während der Anmeldung spontan migrieren, wenn der Benutzer kein Profil im Benutzerspeicher hat. Anschließend verwendet die Profilverwaltung das Profil im Benutzerspeicher in der aktuellen Sitzung und in allen künftigen Sitzungen, die mit dem Pfad zu demselben Benutzerspeicher konfiguriert sind.

Standardmäßig werden lokale Profile und Roamingprofile während der Anmeldung in den Benutzerspeicher migriert.

Um anzugeben welche Profiltypen bei der Anmeldung in den Benutzerspeicher migriert werden sollen, wählen Sie eine der folgenden Optionen:
- Lokal und Roaming
- Lokal
- Roaming
- Keine (deaktiviert)

Wenn Sie Keine auswählen, wird der vorhandene Windows-Mechanismus für die Erstellung neuer Profile verwendet, genau wie in einer Umgebung, in der die Profilverwaltung nicht installiert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale und servergespeicherte Profile migriert.

### Pfad zum Vorlagenprofil

Mit dieser Einstellung geben Sie den Pfad zu dem Profil an, das die Profilverwaltung als Vorlage zum Erstellen neuer Benutzerprofile verwenden soll.

Dies muss der vollständige Pfad zu dem Ordner sein, der die Registrierungsdatei NTUSER.DAT und sämtliche anderen für das Vorlagenprofil erforderlichen Dateien und Ordner enthält.
Hinweis: Geben Sie mit dem Pfad nicht NTUSER.DAT ein. Geben Sie für die Datei \\Server\Profile\Vorlage\ntuser.dat den Speicherort als \\Server\Profile\Vorlage an.
Verwenden Sie einen absoluten Pfad (entweder einen UNC-Pfad oder einen Pfad auf dem lokalen Computer). Sie können einen lokalen Pfad verwenden, um z. B. ein Vorlagenprofil auf einem Citrix Provisioning Services-Image dauerhaft anzugeben. Relative Pfade werden nicht unterstützt.

Hinweis: Beachten Sie, dass diese Richtlinie nicht die Erweiterung von Active Directory-Attributen, Systemumgebungsvariablen oder der Variablen %USERNAME% und %USERDOMAIN% unterstützt.
Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

### Vorlagenprofil überschreibt lokales Profil

Diese Einstellung ermöglicht eine Überschreibung des lokalen Profils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat, aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das lokale Profil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das lokale Profil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

### Vorlagenprofil überschreibt Roamingprofil

Diese Einstellung ermöglicht eine Überschreibung eines Roamingprofils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das Roamingprofil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das Roamingprofil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

### Als verbindliches Citrix Profil für alle Anmeldungen verwendete Vorlagenprofil

Bei Auswahl dieser Einstellung verwendet die Profilverwaltung das Vorlagenprofil als Standardprofil bei der Erstellung aller neuen Benutzerprofile.

Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Registrierung"

Jul 08, 2016

Der Abschnitt "Registrierung" enthält Richtlinieneinstellungen, mit denen Sie festlegen können, welche Registrierungsschlüssel bei der Verarbeitung der Profilverwaltung berücksichtigt und welche ausgeschlossen werden sollen.

## Ausschlussliste

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die nicht von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel von der Verarbeitung ausgeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Registrierungsschlüssel von der Verarbeitung ausgeschlossen.

## Aufnahmeliste

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel in die Verarbeitung eingeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die gesamte HKCU-Struktur verarbeitet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Gestreamte Benutzerprofile"

Jul 08, 2016

Der Abschnitt "Gestreamte Benutzerprofile" enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

## Immer zwischenspeichern

Mit dieser Einstellung geben Sie an, ob die Profilverwaltung gestreamte Dateien so bald wie möglich zwischenspeichern soll, wenn sich ein Benutzer anmeldet. Durch das Zwischenspeichern von Dateien, nachdem sich ein Benutzer anmeldet, wird Netzwerkbandbreite gespart und die Benutzererfahrung optimiert.

Verwenden Sie diese Einstellung mit der Einstellung Profilstreaming.

Standardmäßig ist diese Einstellung deaktiviert und gestreamte Dateien werden nicht so schnell wie möglich zwischengespeichert, wenn sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

## Immer Cachegröße

Mit dieser Einstellung geben Sie eine Untergrenze (in Megabytes) für die Größe der Dateien an, die gestreamt werden. Die Profilverwaltung speichert Dateien dieser Größe bzw. größere Dateien so bald wie möglich zwischen, wenn ein Benutzer sich anmeldet.

Die Standardeinstellung ist 0 (null) und die Funktion zum Zwischenspeichern des gesamten Profils wird verwendet. Wenn das Feature zum Zwischenspeichern des gesamten Profils aktiviert ist, ruft die Profilverwaltung den gesamten Inhalt des Profils im Benutzerspeicher als Hintergrundaufgabe ab, nachdem sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

## Profilstreaming

Diese Einstellung aktiviert oder deaktiviert das Feature für gestreamte Citrix Benutzerprofile. Wenn diese Option aktiviert ist, werden Dateien und Ordner in einem Profil nur dann aus dem Benutzerspeicher auf den lokalen Computer abgerufen, wenn auf sie von Benutzern nach der Anmeldung zugegriffen wird. Registrierungseinträge und Dateien im Bereich für ausstehende Dateien werden sofort abgerufen.

Standardmäßig ist das Profilstreaming ist deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

## Gruppen mit gestreamten Benutzerprofilen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dieser Einstellung geben Sie die Benutzerprofile in einer Organisationseinheit gestreamt werden, basierend auf Windows Benutzergruppen.

Wenn diese Option aktiviert ist, werden nur die Benutzerprofile in den angegebenen Benutzergruppen gestreamt. Alle anderen Benutzerprofile werden normal verarbeitet.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden normal verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

### Timeout für gesperrte Dateien im ausstehenden Bereich

Mit dieser Einstellung geben Sie einen Zeitraum (in Tagen) an, nach dem Dateien der Benutzer aus dem Bereich für ausstehende Dateien in den Benutzerspeicher zurückgeschrieben werden, wenn ein Server nicht mehr reagiert und der Benutzerspeicher gesperrt bleibt. Dies verhindert ein Aufblähen des ausstehenden Bereichs und stellt sicher, dass der Benutzerstore immer die aktuellen Dateien enthält.

Die Standardeinstellung ist 1 Tag.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Receiver"

Jul 08, 2016

Hinweis: Wenn nicht anders angegeben, bezieht sich "Receiver" auf Citrix Receiver.

Der Abschnitt "Receiver" enthält Richtlinieneinstellungen zum Angeben einer Liste von StoreFront-Adressen, die für auf dem virtuellen Desktop ausgeführte Windows-Betriebssysteme per Push an Citrix Receiver für Windows übertragen werden sollen.

## StoreFront-Kontenliste

Mit dieser Einstellung geben Sie eine Liste der StoreFront-Stores an, die Administratoren für die Übertragung per Push an Citrix Receiver für Windows auswählen können. Beim Erstellen einer Bereitstellungsgruppe können Administratoren auswählen, welche Stores für Citrix Receiver für Windows auf virtuellen Desktops, die in dieser Gruppe ausgeführt werden, per Push übertragen werden sollen.

In der Standardeinstellung sind keine Stores angegeben.

Geben Sie für jeden Store die folgenden Informationen in Form eines durch Semikolons getrennten Eintrags an:

- Storename: der Name des Stores wie er Benutzern angezeigt wird.
- Store-URL: die URL des Stores.
- Storeaktivierungszustand: Ob der Store für Benutzer verfügbar ist. Dies ist entweder ein oder aus.
- Store-Beschreibung: die Beschreibung des Stores, die Benutzern angezeigt wird.

Beispiel: Vertriebsstore;https://sales.mycompany.com/Citrix/Store/discovery;On;Store für Vertriebsmitarbeiter


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Virtual Delivery Agent"

Jul 08, 2016

Der Abschnitt "Virtual Delivery Agent" (VDA) enthält Richtlinieneinstellungen, mit denen Sie die Kommunikation zwischen VDA und Controllern einer Site steuern können.

Wichtig: Der VDA benötigt die in diesen Einstellungen enthaltenen Informationen für die Registrierung bei einem Delivery Controller, wenn das Feature für automatische Controllerupdates nicht verwendet wird. Da die Informationen für die Registrierung erforderlich sind, müssen Sie sie mit dem Gruppenrichtlinien-Editor konfigurieren, sofern Sie sie nicht bei der VDA-Installation angeben.

- IPv6-Netzwerkmaske für Controllerregistrierung
- Controllerregistrierungsport
- Controller-SIDs
- Controller
- Nur IPv6-Controllerregistrierung verwenden
- Site-GUID

## IPv6-Netzwerkmaske für Controllerregistrierung

Mit dieser Richtlinieneinstellung kann der VDA auf ein bevorzugtes Subnetz (anstelle einer globalen IP, sofern registriert) limitiert werden. Mit dieser Einstellung geben Sie die IPv6-Adresse und das Netzwerk an, in dem der VDA registriert wird. Der VDA wird nur an der ersten Adresse registriert, die mit der angegebenen Netzmaske übereinstimmt. Diese Einstellung ist nur gültig, wenn die Richtlinieneinstellung Nur IPv6-Controllerregistrierung verwenden aktiviert ist.

Diese Einstellung ist standardmäßig leer.

## Controllerregistrierungsport

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie die TCP/IP-Portnummer an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird.

Die Standardeinstellung der Portnummer ist "80".

## Controller-SIDs

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie eine durch Leerzeichen getrennte Liste von Controller-SIDs an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird. Dies ist eine optionale Einstellung, die mit der Einstellung "Controller" verwendet werden kann, um die für die Registrierung verwendete Liste von Controllern zu beschränken.

Diese Einstellung ist standardmäßig leer.

## Controller

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie eine durch Leerzeichen getrennte Liste von vollständig qualifizierten Domänennamen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

(FQDN) für Controller an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird. Dies ist eine optionale Einstellung, die mit der Einstellung "Controller-SIDs" verwendet werden kann.

Diese Einstellung ist standardmäßig leer.

### Automatische Controllerupdates aktivieren

Mit dieser Einstellung ist eine automatische Registrierung des VDAs bei einem Controller nach der Installation möglich.

Nach der Registrierung wird von dem Controller, bei dem der VDA registriert ist, eine Liste der aktuellen Controller-FQDNs und -SIDs an den VDA gesendet. Diese Liste wird in den persistenten Speicher des VDAs geschrieben. Jeder Controller prüft die Datenbank alle 90 Minuten auf Controllerinformationen. Wurde seit der letzten Prüfung ein Controller hinzugefügt oder entfernt oder ist eine Richtlinienänderung erfolgt, sendet der Controller eine aktualisierte Liste an die bei ihm registrierten VDAs. Der VDA nimmt alle Verbindungen von allen Controllern in der aktuellen Liste an.

Standardmäßig ist diese Einstellung aktiviert.

### Nur IPv6-Controllerregistrierung verwenden

Diese Einstellung steuert die Form der Adresse, die vom VDA für die Registrierung beim Controller verwendet wird:

- Bei aktivierter Einstellung wird der VDA mit der IPv6-Adresse der Maschine für die Kommunikation beim Controller registriert. Wenn der VDA mit dem Controller kommuniziert, wird eine Adresse verwendet, deren Auswahl folgender Reihenfolge unterliegt: globale IP-Adresse, ULA-Adresse, Link-Local-Adresse (wenn keine anderen IPv6-Adressen verfügbar sind).
- Bei deaktivierter Einstellung wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.

Diese Einstellung ist standardmäßig deaktiviert.

### Site-GUID

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Diese Einstellung gibt den Globally Unique Identifier (GUID) der Site an, den der VDA für die Registrierung bei einem Controller verwendet, wenn die Active Directory-basierte Registrierung verwendet wird.

Diese Einstellung ist standardmäßig leer.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "HDX 3D Pro"

Jul 08, 2016

Der Bereich "HDX 3D Pro" enthält Richtlinieneinstellungen, mit denen Sie das Tool zum Konfigurieren der Bildqualität für Benutzer aktivieren und konfigurieren können. Mit dem Tool können Benutzer die Verwendung der verfügbaren Bandbreite durch Anpassen des Verhältnisses zwischen Bildqualität und Reaktionszeit in Echtzeit optimieren.

## Verlustfrei aktivieren

Mit dieser Einstellung wird angegeben, ob Benutzer verlustfreie Komprimierung mit dem Tool zum Konfigurieren der Bildqualität aktivieren oder deaktivieren können. In der Standardeinstellung wird den Benutzern die Möglichkeit zum Aktivieren der verlustfreien Komprimierung nicht eingeräumt.

Aktiviert ein Benutzer die verlustfreie Komprimierung, wird die Bildqualität automatisch auf den höchsten Wert eingestellt, der im Bildkonfigurationstool verfügbar ist. Standardmäßig kann je nach Leistungsfähigkeit des Benutzergeräts und des Hostcomputers entweder die GPU-basierte oder die CPU-basierte Komprimierung verwendet werden.

## HDX3DPro-Qualitätseinstellungen

Mit dieser Einstellung geben Sie den Mindest- und den Höchstwert an, mit denen der Bildqualitätsanpassungsbereich, der den Benutzern im Tool zum Konfigurieren der Bildqualität zur Verfügung steht, festgelegt wird.

Geben Sie für die Bildqualität Werte zwischen 0 und 100 an. Der Höchstwert muss größer oder gleich dem Mindestwert sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Einstellungen der Richtlinie "Virtuelle IP"

Jul 08, 2016

Der Abschnitt "Virtuelle IP" enthält Richtlinieneinstellungen für die Angabe, ob Sitzungen eine eigene virtuelle Loopbackadresse haben.

## Virtuelle IP - Loopbackunterstützung

Wenn diese Einstellung aktiviert ist, hat jede Sitzung eine eigene virtuelle Loopbackadresse. Wenn diese Einstellung deaktiviert ist, haben Sitzungen keine individuellen Loopbackadressen.

Diese Einstellung ist standardmäßig deaktiviert.

## Virtuelle IP - Programme für virtuelles Loopback

Mit dieser Einstellung geben Sie die ausführbaren Dateien der Anwendungen an, die virtuelle Loopbackadressen verwenden können. Wenn Sie der Liste Programme hinzufügen, geben Sie nur den Namen der ausführbaren Datei an. Sie müssen nicht den gesamten Pfad angeben.

In der Standardeinstellung sind keine ausführbaren Dateien angegeben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung

Jul 08, 2016

In den VDA-Versionen 7.0 bis 7.8 können COM- und LPT-Porteinstellungen nur über die Registrierung konfiguriert werden. In VDA-Versionen vor 7.0 und in Version 7.9 können Sie diese Einstellungen in Studio konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Portumleitung" und Einstellungen der Richtlinie "Bandbreite".

Richtlinieneinstellungen für COM-Port- und LPT-Portumleitung befinden sich unter HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated auf dem VDA-Image oder Computer.

Zum Aktivieren der COM-Port- und LPT-Portumleitung, fügen Sie neue Registrierungsschlüssel vom Typ REG_DWORD wie folgt hinzu:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

| Registrierungsschlüssel | Beschreibung | Zulässige Werte |
|---|---|---|
| AllowComPortRedirection | Zulassen oder Verhindern der COM-Portumleitung | 1 (Zulassen) oder 0 (Verhindern) |
| LimitComBw | Bandbreitenlimit für COM-Portumleitungskanal | Numerischer Wert |
| LimitComBWPercent | Bandbreitenlimit für COM-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite | Numerischer Wert zwischen 0 und 100 |
| AutoConnectClientComPorts | Automatische Verbindung von COM-Ports auf dem Benutzergerät | 1 (Zulassen) oder 0 (Verhindern) |
| AllowLptPortRedirection | Zulassen oder Verhindern der LPT-Portumleitung | 1 (Zulassen) oder 0 (Verhindern) |
| LimitLptBw | Bandbreitenlimit für LPT-Portumleitungskanal | Numerischer Wert |
| LimitLptBwPercent | Bandbreitenlimit für LPT-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite | Numerischer Wert zwischen 0 und 100 |
| AutoConnectClientLptPorts | Automatische Verbindung von LPT-Ports auf dem Benutzergerät | 1 (Zulassen) oder 0 (Verhindern) |

Nach dem Konfigurieren dieser Einstellungen ändern Sie die Maschinenkataloge, damit sie das neue Masterimage oder die aktualisierte physische Maschine verwenden. Wenn sich die Benutzer das nächste Mal abmelden, werden die Desktops mit den neuen Einstellungen aktualisiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Richtlinieneinstellungen für Connector für Configuration Manager 2012

Jul 08, 2016

Der Abschnitt "Connector für Configuration Manager 2012" enthält Richtlinieneinstellungen zum Konfigurieren des Citrix Connector 7.5-Agents.

Wichtig: Richtlinien für Warnungs-, Abmeldungs- und Neustartmeldungen gelten nur für Bereitstellungen für Serverbetriebssystemmaschinenkataloge, die manuell oder über Provisioning Services verwaltetet werden. Bei solchen Maschinenkatalogen benachrichtigt der Connector-Dienst Benutzer über ausstehende Anwendungsinstallationen oder Softwareupdates.
Verwenden Sie bei über MCS verwalteten Katalogen Studio zur Benachrichtigung der Benutzer. Verwenden Sie bei manuell verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Configuration Manager zur Benachrichtigung der Benutzer. Verwenden Sie bei mit Provisioning Services verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Provisioning Services zur Benachrichtigung der Benutzer.

## Zeitraum für Vorabwarnung

Diese Einstellung gibt das Intervall an, mit dem Benutzern Vorabmeldungen angezeigt werden.

Intervalle werden im Format ttt.hh:mm:ss festgelegt. Dabei gilt Folgendes:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

Das Standardintervall ist 1 Stunde (01:00:00).

## Meldungsfeldtext für Vorabwarnung

Diese Einstellung enthält den editierbaren Text für die Vorabmeldung, die Benutzer vor anstehenden Softwareupdates oder Wartungsaufgaben erhalten, für die sie sich abmelden müssen.

Die Standardmeldung lautet: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

## Meldungsfeldtitel für Vorabwarnung

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der Vorabmeldung, die Benutzer erhalten.

Der Standardtitel ist: Upcoming Maintenance

## Zeitraum für Vorabwarnung

Diese Einstellung definiert, wie lange vor Wartungsaufgaben die Vorabwarnmeldung zum ersten Mal angezeigt wird.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist der Wert 16 Stunden (16:00:00), d. h. dass die erste Vorabwarnmeldung ca. 16 Stunden vor der Wartung angezeigt wird.

### Letzter Meldungsfeldtext für Abmeldung erzwingen

Diese Einstellung enthält den editierbaren Text für die Meldung, die Benutzer warnt, dass die Abmeldung erzwungen wird.

Die Standardmeldung lautet: The server is currently going offline for maintenance

### Letzter Meldungsfeldtitel für Abmeldung erzwingen

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der letzten Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

### Kulanzzeitraum für erzwungenes Abmelden

Diese Einstellung definiert den Kulanzzeitraum, der Benutzern zugestanden wird, nachdem sie gewarnt wurden, dass die Abmeldung erzwungen wird, und dem tatsächlichen erzwungenen Abmelden, damit die ausstehenden Wartungsaufgaben gestartet werden können.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:
- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist der Kulanzzeitraum für erzwungenes Abmelden auf 5 Minuten (00:05:00) festgelegt.

### Letzter Meldungsfeldtext für Abmeldung erzwingen

Diese Einstellung enthält den editierbaren Text für die letzte Warnmeldung, die Benutzer auffordert, ihre Arbeit zu speichern und sich vor der erzwungenen Abmeldung abzumelden.

Die Standardmeldung enthält den folgenden Text: "{TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}

### Meldungsfeldtitel für Abmeldung erzwingen

Diese Einstellung enthält den editierbaren Text für die Titelleiste der Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

### Imageverwalteter Modus

Der Connector-Agent erkennt automatisch, wenn er auf einem von Provisioning Services oder MCS verwalteten Maschinenklon ausgeführt wird. Der Agent blockiert Configuration Manager-Updates auf imageverwalteten Klonen und installiert die Updates automatisch auf dem Masterimage des Katalogs.

Nachdem ein Masterimage aktualisiert wurde, verwenden Sie Studio zum Orchestrieren des Neustarts der MCS-Klone. Der Connector-Agent orchestriert automatisch den Neustart von PVS-Katalogklonen während der Configuration Manager-Wartung. Zur Außerkraftsetzung dieses Verhaltens, damit Software auf Katalogklonen von Configuration Manager

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

installiert wird, ändern Sie den Modus von "Imageverwaltet" in Deaktiviert.

### Meldungsfeldtext für Neustarten

Diese Einstellung enthält den editierbaren Text der Benutzermeldung, dass der Server bald neu gestartet wird.

Die Standardmeldung lautet: The server is currently going offline for maintenance

### Normales Zeitintervall, in dem die Agent-Aufgabe ausgeführt wird

Durch diese Einstellung wird festgelegt, wie häufig der Citrix Connector Agent-Aufgabe ausgeführt wird.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist das Intervall auf fünf Minuten (00:05:00) festgelegt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwaltung

Jul 08, 2016

Die Verwaltung einer XenApp- oder XenDesktop-Site hat vielfältige Aspekte.

### Lizenzierung

Eine gültige Verbindung mit dem Citrix Lizenzserver ist zum Erstellen einer Site erforderlich. Anschließend können Sie Aufgaben wie das Hinzufügen von Lizenzen, das Ändern von Lizenztyp oder -modell und das Verwalten von Lizenzadministratoren über Studio erledigen. Über Studio können Sie auch auf die License Administration Console zugreifen.

### Anwendungen

Anwendungen werden in Bereitstellungsgruppen und optional in Anwendungsgruppen verwaltet.

### Zonen

In geografisch verteilten Bereitstellungen führen Sie Anwendungen und Desktops mithilfe von Zonen näher am Benutzer, um die Leistung zu verbessern. Beim Installieren und Konfigurieren einer Site sind alle Controller, Maschinenkataloge und Hostverbindungen in der primären Zone. Später können Sie mit Studio Satellitenzonen für diese Elemente erstellen. Wenn Sie mehrere Zonen haben, können Sie angeben, in welcher Zone neu erstellte Maschinenkataloge, Hostverbindungen und Controller hinzugefügt werden sollen. Sie können Elemente auch zwischen Zonen verschieben.

### Verbindungen und Ressourcen

Wenn die Maschinen, über die Anwendungen und Desktops für Benutzer bereitgestellt werden, von einem Hypervisor oder Clouddienst gehostet werden, richten Sie die erste Verbindung beim Erstellen einer Site mit dem Hypervisor bzw. Clouddienst ein. Die Speicher- und Netzwerkdetails dieser Verbindung sind ihre *Ressourcen*. Später können Sie die Verbindung und ihre Ressourcen ändern und neue Verbindungen erstellen. Sie können auch die Maschinen verwalten, die eine konfigurierte Verbindung verwenden.

### Verbindungsleasing

Das Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist. Das Verbindungsleasing kann zwar die Verbindungsresilienz und die Produktivität der Benutzer verbessern, es sind jedoch Überlegungen im Hinblick auf Verfügbarkeit, Betrieb und Leistung anderer Funktionen anzustellen. Diese werden im vorliegenden Artikel behandelt.

### Virtuelle IP-Adressen und virtuelles Loopback

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

### Delivery Controller

Bevor ein VDA die Bereitstellung von Anwendungen und Desktops unterstützen kann, muss er bei einem Controller zum Aufbau der Kommunikation registriert werden. Controlleradressen können bei der Installation eines VDAs, über Citrix


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Richtlinieneinstellungen oder Registrierungseinstellungen und auf andere Weise angegeben werden. Es ist wichtig, dass die VDAs beim Hinzufügen, Verschieben und Entfernen von Controllern immer aktualisierte Informationen erhalten. In diesem Abschnitt wird beschrieben, wie und wann VDAs registriert werden, wie die Controllerinformationen aktualisiert werden und wie Controller hinzugefügt, verschoben und entfernt werden.

### Sitzungen

Das Erhalten der Sitzungsaktivität ist wichtig, um eine optimale Benutzererfahrung zu gewährleisten. Mit diversen Features können Sie die Sitzungszuverlässigkeit optimieren und damit das Risiko von Problemen, Ausfallzeiten und Produktivitätsverlusten verringern.

- Sitzungszuverlässigkeit
- Automatische Wiederverbindung von Clients
- ICA-Keep-Alive
- Workspace Control
- Sitzungsroaming

### Durchführung einer Suche in Studio

Zum Anzeigen von Informationen zu Maschinen, Sitzungen, Maschinenkatalogen, Anwendungen und Bereitstellungsgruppen in Studio steht ein flexibles Suchfeature zur Verfügung.

### Tags

Tags werden zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Gruppen und Richtlinien verwendet. Sie können Vorgänge mit einem Tag konfigurieren, sodass sie auf spezifische Objekte angewendet werden.

### IPv4/ipv6

Dieses Release von XenApp und XenDesktop unterstützt reines IPv4, reines IPv6a und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden. In diesem Abschnitt werden solche Bereitstellungen beschrieben. Außerdem werden die Citrix Richtlinieneinstellungen vorgestellt, mit denen die Verwendung von IPv4 bzw. IPv6 gesteuert wird.

### Clientordnerumleitung

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Windows-Desktopgerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

### Benutzerprofile

Standardmäßig wird die Citrix Profilverwaltung automatisch zusammen mit einem VDA installiert. Wenn Sie diese Lösung verwenden, lesen Sie diesen Artikel mit allgemeinen Hinweisen und die Dokumentation zur Profilverwaltung mit umfassenden Informationen.

### Citrix Insight Services

Citrix Insight Services (CIS) ist eine Plattform von Citrix für Instrumentierung, Telemetrie und Ablaufverfolgung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Lizenzierung

Jul 08, 2016

Sie können die Lizenzierung in Studio verwalten und nachverfolgen, wenn der Lizenzserver in derselben Domäne wie Studio oder in einer vertrauenswürdigen Domäne ist. Informationen zu anderen Lizenzierungsaufgaben finden Sie in der Dokumentation zur Lizenzierung.

Sie müssen für die nachfolgend beschriebenen Aufgaben Volladministrator für die Lizenzierung sein, außer um die Lizenzinformationen anzuzeigen. Zum Anzeigen der Lizenzinformationen in Studio muss der Administrator mindestens Lesezugriff als delegierter Administrator für die Lizenzierung haben. Die integrierten Rollen des Volladministrators und des Administrators mit Leserechten haben diese Berechtigung.

In der folgenden Tabelle werden die unterstützten Editionen und Lizenzierungsmodelle aufgeführt:

| Produkte | Editionen | Lizenzmodelle |
|---|---|---|
| XenApp | • Platinum<br>• Enterprise<br>• Advanced | CCU |
| XenDesktop | • Platinum<br>• Enterprise<br>• App<br>• VDI | • Benutzer/Gerät<br>• CCU |

Zum Anzeigen der Lizenzinformationen wählen Sie **Konfiguration > Lizenzierung** im Studio-Navigationsbereich. Eine Zusammenfassung der Lizenzverwendung sowie Einstellungen für die Site werden zusammen mit einer Liste aller Lizenzen angezeigt, die aktuell auf dem angegebenen Lizenzserver installiert sind.

Herunterladen einer Lizenz von Citrix:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen zuteilen**.
3. Geben Sie den Lizenzzugangscode an, der per E-Mail von Citrix bereitgestellt wird.
4. Wählen Sie ein Produkt und klicken Sie auf **Lizenzen zuteilen**. Alle Lizenzen, die für das Produkt verfügbar sind, sind zugeteilt und heruntergeladen. Wenn Sie alle Lizenzen für einen bestimmten Lizenzzugangscode zuteilen und herunterladen, können Sie den Lizenzzugangscode nicht erneut verwenden. Zum Durchführen weiterer Transaktionen mit diesem Code melden Sie sich bei My Account an.

Hinzufügen von Lizenzen, die auf dem lokalen Computer oder im Netzwerk gespeichert sind:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen hinzufügen**.
3. Navigieren Sie zu einer Lizenzdatei und fügen Sie sie dem Lizenzserver hinzu.

Ändern des Lizenzservers:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie im Aktionsbereich **Lizenzserver ändern**.
3. Geben Sie die Adresse des Lizenzservers im Format name:port an ("name" = DNS-, NetBIOS- oder IP-Adresse). Wenn Sie keine Portnummer angeben, wird der Standardport (27000) verwendet.

Auswählen des Lizenztyps:

- Beim Konfigurieren der Site werden Sie nach Angabe des Lizenzservers aufgefordert, den zu verwendenden Lizenztyp auszuwählen. Stehen auf dem Server keine Lizenzen zur Verfügung, wird automatisch die Option zur Verwendung des Produkts während einer 30-tägigen Testphase ohne Lizenz ausgewählt.
- Stehen auf dem Server Lizenzen zur Verfügung, werden die entsprechenden Informationen angezeigt. Der Benutzer kann dann die gewünschte Lizenz auswählen. Alternativ können Sie dem Server eine Lizenzdatei hinzufügen und diese dann auswählen.

Ändern von Produktedition und Lizenzierungsmodell:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Produktedition bearbeiten**.
3. Aktualisieren Sie die entsprechenden Optionen.

Zum Öffnen der License Administration Console wählen Sie im Aktionsbereich **License Administration Console**. Die Konsole wird normalerweise sofort angezeigt. Wenn das Dashboard jedoch mit Kennwortschutz konfiguriert wurde, werden Sie aufgefordert, die Anmeldeinformationen für die License Administration Console einzugeben. Informationen zur Verwendung der Konsole finden Sie in der Dokumentation zur Lizenzierung.

Hinzufügen eines Lizenzadministrators:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im mittleren Bereich die Registerkarte Lizenzierungsadministratoren.
3. Wählen Sie im Aktionsbereich **Lizenzadministrator hinzufügen**.
4. Navigieren Sie zu dem Benutzer, den Sie als Administrator hinzufügen möchten, und wählen Sie die Berechtigungen.

Ändern der Berechtigungen eines Lizenzadministrators oder Löschen eines Lizenzadministrators

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie die Registerkarte Lizenzadministratoren im mittleren Bereich und dann den Lizenzadministrator.
3. Wählen Sie im Aktionsbereich **Lizenzadministrator bearbeiten** bzw. **Lizenzadministrator löschen**.

Hinzufügen einer Lizenzadministratorgruppe:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im mittleren Bereich die Registerkarte Lizenzierungsadministratoren.
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe hinzufügen**.
4. Navigieren Sie zu der Gruppe, deren Mitglieder Sie als Administratoren hinzufügen möchten, und wählen Sie die Berechtigungen. Beim Hinzufügen einer Active Directory-Gruppe werden den Benutzern dieser Gruppe Lizenzierungsadministratorberechtigungen erteilt.

Ändern der Berechtigungen einer Lizenzierungsadministratorengruppe oder Löschen einer Lizenzierungsadministratorengruppe

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie die Registerkarte Lizenzadministratoren im mittleren Bereich und dann die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Lizenzierungsadministratorengruppe.

3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe bearbeiten** bzw. **Lizenzierungsadministratorengruppe löschen**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anwendungen

Jul 08, 2016

# Einführung

Wenn in Ihrer Bereitstellung nur Bereitstellungsgruppen (und keine Anwendungsgruppen) verwendet werden, fügen Sie den Bereitstellungsgruppen Anwendungen hinzu. Wenn Sie auch Anwendungsgruppen verwenden, sollten Sie die Anwendungen den Anwendungsgruppen hinzufügen. Diese Vorgehensweise vereinfacht die Verwaltung. Eine Anwendung muss immer zu mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe gehören.

Im Assistenten zum Hinzufügen von Anwendungen können Sie Bereitstellungsgruppen oder Anwendungsgruppen auswählen, aber nicht beides. Sie können zwar später die Gruppenzuordnung einer Anwendung ändern (z. B. können Sie eine Anwendung von einer Anwendungsgruppe in eine Bereitstellungsgruppe verschieben), jedoch wird vom Hinzufügen dieser Komplexität abgeraten. Ihre Anwendungen sollten in einem Gruppentyp sein.

Wenn Sie eine Anwendung mehreren Bereitstellungsgruppen oder Anwendungsgruppen zuordnen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Bereitstellungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Gruppen, denen die Anwendung zugeordnet wurde.

Wenn Sie zwei Anwendungen mit dem gleichen Namen (möglicherweise aus verschiedenen Gruppen) den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft "Anwendungsname (Benutzer)", sonst wird den Benutzern der Name in Citrix Receiver doppelt angezeigt.

Sie können Anwendungseigenschaften (Einstellungen) beim Hinzufügen oder später ändern. Beim Hinzufügen der Anwendung oder später können Sie zudem den Anwendungsordner ändern, in dem die Anwendung gespeichert wird.

Weitere Informationen:

- Informationen zu Bereitstellungsgruppen finden Sie unter Erstellen von Bereitstellungsgruppen.
- Informationen zu Anwendungsgruppen finden Sie unter Erstellen von Anwendungsgruppen.
- Informationen zu Tags, die Sie Anwendungen hinzufügen können, finden Sie unter Tags.

# Hinzufügen von Anwendungen

Beim Erstellen einer Bereitstellungsgruppe oder Anwendungsgruppe können Sie der Gruppe Anwendungen hinzufügen. Die dazu erforderlichen Schritte werden in den Artikeln "Erstellen von Bereitstellungsgruppen" und "Erstellen von Anwendungsgruppen" beschrieben. Im Folgenden wird beschrieben, wie Sie Anwendungen nach dem Erstellen einer Gruppe hinzufügen.

Gut zu wissen:

- Sie können Remote-PC-Zugriff-Bereitstellungsgruppen keine Anwendungen hinzufügen.
- Sie können mit dem Assistenten zum Hinzufügen von Anwendungen keine Anwendungen aus Bereitstellungsgruppen oder Anwendungsgruppen entfernen. Dies ist ein separater Vorgang.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinzufügen von Anwendungen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann im Aktionsbereich **Anwendungen hinzufügen**.
2. Der Assistent zum Hinzufügen von Anwendungen wird mit der Seite **Einführung** gestartet. Diese Seite können Sie für künftige Starts des Assistenten unterdrücken.
3. Der Assistent führt Sie durch die im Folgenden beschriebenen Seiten "Gruppen", "Anwendungen" und "Zusammenfassung". Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur Seite "Zusammenfassung" gelangen.

Alternativen für Schritt 1, wenn Sie Anwendungen einer einzelnen Bereitstellungsgruppe oder Anwendungsgruppe hinzufügen möchten:

- Zum Hinzufügen von Anwendungen zu einer Bereitstellungsgruppe wählen Sie in Schritt 1 im Studio-Navigationsbereich **Bereitstellungsgruppe**, wählen Sie dann im mittleren Bereich eine Bereitstellungsgruppe und im Aktionsbereich **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.
- Zum Hinzufügen von Anwendungen zu einer Anwendungsgruppe wählen Sie in Schritt 1 im Studio-Navigationsbereich **Anwendungen**, wählen Sie dann im mittleren Bereich eine Anwendungsgruppe aus und wählen Sie im Aktionsbereich unter dem Namen der Anwendungsgruppe den Eintrag **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.

## Gruppen

Auf dieser Seite werden alle Bereitstellungsgruppen der Site aufgelistet. Wenn Sie auch Anwendungsgruppen erstellt haben, werden die Anwendungsgruppen und Bereitstellungsgruppen aufgeführt. Sie können in einer der Gruppen eine Auswahl treffen, aber nicht in beiden Gruppen. Das heißt, Sie können Anwendungen nicht gleichzeitig einer Anwendungsgruppe und einer Bereitstellungsgruppe hinzufügen. Im Allgemeinen gilt, wenn Sie Anwendungsgruppen verwenden, sollten Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt werden.

Beim Hinzufügen einer Anwendung müssen Sie das Kontrollkästchen mindestens einer Bereitstellungsgruppe (oder Anwendungsgruppe, falls verfügbar) aktivieren, da eine Anwendung immer mindestens einer Gruppe zugeordnet sein muss.

## Anwendungen

Klicken Sie auf die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

| Quelle | Beschreibung |
|---|---|
| Vom Startmenü | Anwendungen, die auf einer Maschine in den ausgewählten Bereitstellungsgruppen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der Anwendungen, die hinzugefügt werden sollen, und klicken Sie auf **OK**.<br><br>Diese Quelle kann nicht ausgewählt werden, wenn Sie (1) Anwendungsgruppen gewählt haben, denen keine Bereitstellungsgruppen zugeordnet sind, (2) Anwendungsgruppen gewählt haben, deren zugeordnete Bereitstellungsgruppen keine Maschinen enthalten, oder (3) eine Bereitstellungsgruppe gewählt haben, die keine Maschinen enthält. |
| Manuell | Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **OK**. |
| Vorhandene | Anwendungen, die der Site zuvor hinzugefügt wurden. Wenn Sie diese Quelle auswählen, wird eine neue Seite mit einer Liste der erkannten Anwendungen gestartet. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**.<br><br>Diese Quelle kann nicht ausgewählt werden, wenn die Site keine Anwendungen enthält. |
| App-V | Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Aktivieren Sie daraufhin die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Weitere Informationen finden Sie im Artikel über App-V.<br><br>Diese Quelle kann nicht ausgewählt werden, wenn App-V nicht für die Site konfiguriert ist. |
| Anwendungsgruppe | Anwendungsgruppen: Wenn Sie diese Quelle auswählen, wird eine neue Seite mit einer Liste der Anwendungsgruppen gestartet. (Zwar werden auch die Anwendungen jeder Gruppe angezeigt, aber Sie können nur die Gruppe, nicht die einzelnen Anwendungen auswählen.) Alle aktuellen und zukünftigen Anwendungen in den ausgewählten Gruppen werden hinzugefügt. Aktivieren Sie die Kontrollkästchen der Anwendungsgruppen, die Sie hinzufügen möchten, und klicken Sie auf **OK**.<br><br>Diese Quelle kann nicht ausgewählt werden, (1) wenn keine Anwendungsgruppen vorhanden sind oder (2) wenn die ausgewählten Bereitstellungsgruppen keine Anwendungsgruppen unterstützen (z. B. Bereitstellungsgruppen mit statisch zugewiesenen Maschinen). |

In der Tabelle wurde schon darauf hingewiesen, dass einige Quellen in der Dropdownliste "Hinzufügen" nicht ausgewählt werden können, wenn keine gültige Quelle des Typs vorhanden ist. Quellen, die nicht kompatibel sind (z. B. können Sie Anwendungsgruppen keine Anwendungsgruppen hinzufügen), werden nicht in der Dropdownliste angezeigt. Anwendungen, die den ausgewählten Gruppen bereits hinzugefügt wurden, können nicht ausgewählt werden.

Sie können die Eigenschaften einer Anwendung (Einstellungen) auf dieser Seite oder später ändern.

Standardmäßig werden hinzugefügte Anwendungen in einem Anwendungsordner mit dem Namen "Applications" abgelegt. Sie können die Anwendung auf dieser Seite oder später ändern. Wenn Sie eine Anwendung hinzufügen und es bereits eine Anwendung mit dem gleichen Namen im gleichen Ordner gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Übernehmen Sie den angebotenen neuen Namen oder lehnen Sie ihn ab und benennen Sie die Anwendung um oder wählen Sie einen anderen Ordner. Wenn beispielsweise "App" im Ordner "Applications" bereits vorhanden ist und Sie versuchen, dem Ordner eine andere Anwendung mit demselben Namen hinzuzufügen, wird der neue Name "App_1" angeboten.

## Zusammenfassung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn Sie 10 oder weniger Anwendungen hinzufügen, werden ihre Namen in in der Liste **Hinzuzufügende Anwendungen** aufgeführt. Wenn Sie mehr als 10 Anwendungen hinzufügen, wird die Gesamtzahl angegeben.

Lesen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.

# Ändern der Gruppenzuordnung einer Anwendung

Nach dem Hinzufügen einer Anwendung können Sie die Bereitstellungsgruppen und Anwendungsgruppen ändern, denen die Anwendung zugeordnet ist.

Mit Drag & Drop können Sie eine Anwendung einer zusätzlichen Gruppe zuordnen. Dies ist eine Alternative zum Verwenden der Befehle im Aktionsbereich.

Wenn eine Anwendung mehr als einer Bereitstellungsgruppe oder mehr als einer Anwendungsgruppe zugeordnet ist, können Sie mit der Gruppenpriorität die Reihenfolge angeben, in der Gruppen nach Anwendungen durchsucht werden. Standardmäßig haben alle Gruppen Priorität 0 (die höchste Priorität). Für Gruppen mit derselben Priorität erfolgt Lastausgleich.

Eine Anwendung kann Bereitstellungsgruppen zugeordnet sein, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten. Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, (1) wenn die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren Version von XenDesktop 7.x erstellt wurde, und (2) wenn Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen" konvertiert, wenn für das Eigenschaftendialogfeld ein Commit ausgeführt wird.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann im mittleren Bereich die Anwendung.
2. Wählen Sie im Aktionsbereich **Eigenschaften**.
3. Wählen Sie die Seite **Gruppen** aus.
4. Zum Hinzufügen einer Gruppe klicken Sie auf die Dropdownliste **Hinzufügen** und wählen Sie **Anwendungsgruppen** oder **Bereitstellungsgruppen**. (Wenn Sie keine Anwendungsgruppen erstellt haben, werden nur Bereitstellungsgruppen angezeigt.) Wählen Sie dann mindestens eine verfügbare Gruppe. Gruppen, die mit der Anwendung nicht kompatibel oder der Anwendung bereits zugeordnet sind, können nicht ausgewählt werden.
5. Zum Entfernen von Gruppen wählen Sie mindestens eine Gruppe aus und klicken Sie auf **Entfernen**. Wenn das Löschen einer Gruppenzuordnung dazu führt, dass die Anwendung keiner Anwendungsgruppe oder Bereitstellungsgruppe mehr zugeordnet ist, werden Sie vor dem Löschen der Anwendung gewarnt.
6. Sie ändern die Priorität einer Gruppe, indem Sie die Gruppe auswählen und dann auf **Priorität bearbeiten** klicken. Wählen Sie einen Wert für die Priorität aus und klicken Sie auf **OK**.
7. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Dialogfeld geschlossen wird.

# Duplizieren, Aktivieren, Deaktivieren, Umbenennen und Löschen von Anwendungen

Folgende Aktionen sind verfügbar:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Duplizieren**: Sie können Anwendungen duplizieren, um eine Anwendungsversion mit anderen Parametern oder Eigenschaften zu erstellen. Wenn Sie eine Anwendung duplizieren, wird diese automatisch mit einem eindeutigen Suffix umbenannt und neben die ursprüngliche Anwendung platziert. Sie können eine Anwendung auch duplizieren und einer anderen Gruppe hinzufügen. (Neben dem Duplizieren ist die einfachste Möglichkeit zum Verschieben einer Datei Drag & Drop.)
- **Aktivieren oder Deaktivieren**: Das Aktivieren und Deaktivieren einer Anwendung ist eine andere Aktion als das Aktivieren und Deaktivieren einer Bereitstellungsgruppe oder Anwendungsgruppe.
- **Umbenennen**: Sie können jeweils nur eine Anwendung umbenennen. Wenn Sie eine Anwendung umbenennen und eine Anwendung mit demselben Namen ist bereits im gleichen Ordner oder in der gleichen Gruppe vorhanden, dann werden Sie aufgefordert, einen anderen Namen anzugeben.
- **Löschen**: Beim Löschen einer Anwendung wird sie aus den Bereitstellungsgruppen und Anwendungsgruppen entfernt, denen sie zugeordnet war, aber nicht aus der Quelle, aus der die Anwendung ursprünglich hinzugefügt wurde. Das Löschen einer Anwendung ist nicht dasselbe wie das Entfernen einer Anwendung aus einer Bereitstellungsgruppe oder Anwendungsgruppe.

Duplizieren, Aktivieren, Deaktivieren, Umbenennen und Löschen von Anwendungen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie mindestens eine Anwendung im mittleren Bereich aus und dann die gewünschte Aufgabe im Aktionsbereich.
3. Bestätigen Sie die Aktion, wenn Sie dazu aufgefordert werden.

# Entfernen von Anwendungen aus einer Bereitstellungsgruppe

Eine Anwendung muss mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Wenn Sie versuchen, eine Anwendung aus einer Bereitstellungsgruppe zu entfernen und dies bedeuten würde, dass die Anwendung keiner Bereitstellungsgruppe oder Anwendungsgruppe mehr zugeordnet wäre, werden Sie gewarnt, dass die Anwendung gelöscht wird, wenn Sie fortfahren. Wenn die Anwendung gelöscht wird und Sie möchten sie bereitstellen, müssen Sie die Anwendung erneut aus einer gültigen Quelle hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe aus. Wählen Sie im mittleren Bereich unten die Registerkarte **Anwendungen** und dann die Anwendung, die Sie entfernen möchten.
3. Wählen Sie im Aktionsbereich **Anwendung entfernen**.
4. Bestätigen Sie das Entfernen.

# Entfernen von Anwendungen aus einer Anwendungsgruppe

Eine Anwendung muss mindestens zu einer Bereitstellungsgruppe oder Anwendungsgruppe gehören. Wenn Sie versuchen, eine Anwendung aus einer Anwendungsgruppe zu entfernen und dies bedeuten würde, dass die Anwendung keiner Bereitstellungsgruppe oder Anwendungsgruppe mehr zugeordnet wäre, werden Sie gewarnt, dass die Anwendung gelöscht wird, wenn Sie fortfahren. Wenn die Anwendung gelöscht wird und Sie möchten sie bereitstellen, müssen Sie die


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Anwendung erneut aus einer gültigen Quelle hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich die Anwendungsgruppe und wählen Sie dann mindestens eine Anwendung aus.
3. Wählen Sie im Aktionsbereich **Aus Anwendungsgruppe entfernen**.
4. Bestätigen Sie das Entfernen.

# Ändern der Anwendungseigenschaften

Sie können jeweils nur die Eigenschaften einer Anwendung ändern.

Ändern der Eigenschaften einer Anwendung

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie die Anwendung und dann im Aktionsbereich **Anwendungseigenschaften bearbeiten**.
3. Wählen Sie die Seite mit der Eigenschaft, die Sie ändern möchten.
4. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

| **Eigenschaft** | **Seite** |
|---|---|
| Kategorie/Ordner, in der/dem die Anwendung in Receiver angezeigt wird | Bereitstellung |
| Befehlszeilenargumente | Speicherort |
| Bereitstellungsgruppen und Anwendungsgruppen, in denen die Anwendung verfügbar ist | Gruppen |
| Beschreibung | Identifizierung |
| Dateinamenerweiterungen und Dateitypzuordnung: die Erweiterungen, die von der Anwendung automatisch geöffnet werden | Dateitypzuordnung |
| Symbol | Bereitstellung |
| Schlüsselwörter für StoreFront | Identifizierung |
| Limits (weitere Informationen finden Sie unter "Konfigurieren von Anwendungslimits") | Bereitstellung |
| | |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Name: die Namen, die Benutzer und Administrator sehen | Identifizierung |
| Pfad zur ausführbaren Datei | Speicherort |
| Verknüpfung auf dem Desktop des Benutzers: aktivieren oder deaktivieren | Bereitstellung |
| Sichtbarkeit: Legt fest, welche Benutzer die Anwendung in Citrix Receiver sehen (eine unsichtbare Anwendung kann trotzdem gestartet werden; damit sie auch nicht verfügbar ist, fügen Sie sie einer anderen Gruppe hinzu) | Sichtbarkeit beschränken |
| Arbeitsverzeichnis | Speicherort |

Anwendungsänderungen werden evtl. für aktuelle Anwendungsbenutzer erst wirksam, wenn diese ihre Sitzung abmelden.

# Konfigurieren von Anwendungslimits

Durch Konfigurieren von Anwendungslimits können Sie die Anwendungsnutzung verwalten. Sie können z. B. die Zahl der Benutzer, die gleichzeitig auf eine Anwendung zugreifen, beschränken. Analog dazu können Sie über Anwendungslimits die Zahl gleichzeitiger Instanzen ressourcenintensiver Anwendungen limitieren, um die Serverleistung zu gewährleisten und eine Dienstverschlechterung zu vermeiden.

**Wichtig:** Diese Funktion limitiert die Anzahl der vom Controller vermittelten Anwendungsstarts (z. B. von Citrix Receiver und StoreFront) und nicht die Anzahl ausgeführter Anwendungen, die auf andere Weise gestartet werden konnten. Anwendungslimits helfen daher bei der Verwaltung der gleichzeitigen Nutzung, gestatten jedoch nicht in allen Szenarios eine Erzwingung. Anwendungslimits können beispielsweise nicht angewendet werden, wenn der Controller eine geleaste Verbindung hat.

Standardmäßig besteht kein Limit für die Anzahl gleichzeitig ausgeführter Anwendungsinstanzen. Sie können eines oder auch beide der zwei möglichen Anwendungslimits konfigurieren:

- Maximale Anzahl gleichzeitiger Instanzen einer Anwendung für alle Benutzer in der Bereitstellungsgruppe
- Eine Anwendungsinstanz pro Benutzer in der Bereitstellungsgruppe

Wenn ein Limit konfiguriert ist und ein Benutzer versucht, eine Anwendungsinstanz zu starten, durch die das Limit überschritten würde, wird eine Fehlermeldung generiert.

Beispiele für Anwendungslimits:

- **Maximale Anzahl gleichzeitiger Instanzen:** Sie konfigurieren für eine Bereitstellungsgruppe die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Alpha" mit 15. Anschließend werden in der Bereitstellungsgruppe 15 Instanzen dieser Anwendung gleichzeitig ausgeführt. Versucht nun ein Benutzer in der Bereitstellungsgruppe, Alpha zu


© 1999-2017 Citrix Systems, Inc. All rights reserved.

starten, wird eine Fehlermeldung generiert und Alpha wird nicht gestartet, da hierdurch das konfigurierte Limit von 15 überschritten würde.

- **Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe haben Sie für die Anwendung "Beta" das Limit von einer Instanz pro Benutzer festgelegt. Benutzer Hermann startet die Anwendung Beta. Eine Weile später versucht er eine weitere Instanz von Beta zu starten. Eine Fehlermeldung wird generiert und Beta wird nicht gestartet, da dadurch das Limit überschritten würde.
- **Maximale Anzahl gleichzeitiger Instanzen plus Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe legen Sie die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Delta" auf 10 fest und aktivieren außerdem das Limit von einer Instanz pro Benutzer. Werden anschließend alle 10 Instanzen von Delta ausgeführt, wird bei jedem weiteren Versuch, die Anwendung in der Bereitstellungsgruppe zu starten, eine Fehlermeldung angezeigt und Delta nicht gestartet. Versucht ein Benutzer, der bereits eine Delta-Instanz gestartet hat, eine zweite Instanz zu starten, wird eine Fehlermeldung angezeigt und die zweite Instanz wird nicht gestartet.

Werden Anwendungsinstanzen auch über andere Methoden als das Controllerbrokering gestartet (z. B. wenn ein Controller eine geleaste Verbindung hat) und die festgelegten Limits werden überschritten, können Benutzer erst dann wieder Instanzen starten, wenn zuvor entsprechend viele Instanzen geschlossen wurden und kein Limit mehr überschritten wird. Die Instanzen, die das Limit überschreiten, werden nicht zwangsweise geschlossen, sondern können weiterlaufen, bis die Benutzer sie schließen.

Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch das Limit einer Anwendungsinstanz pro Benutzer. Wenn Sie das Limit einer Anwendungsinstanz pro Benutzer aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden. Weitere Informationen zum Roaming finden Sie im Artikel Sitzungen.

Konfigurieren von Anwendungslimits

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann eine Anwendung.
2. Wählen Sie im Aktionsbereich **Anwendungseigenschaften bearbeiten**.
3. Wählen Sie auf der Seite **Bereitstellung** eine der folgenden Optionen aus. Wenn Sie fertig sind, klicken Sie auf **OK** oder **Anwenden**. (Mit **OK** werden die Änderungen angewendet und das Dialogfeld "Anwendungseigenschaften bearbeiten" wird geschlossen, mit **Anwenden** werden die Änderungen angewendet und das Dialogfeld bleibt geöffnet.)

- Uneingeschränkte Verwendung der Anwendung zulassen: Es gibt kein Limit für die Anzahl der gleichzeitig ausgeführten Instanzen. Dies ist die Standardeinstellung.
- Limit festlegen: Es sind zwei Limits, die Sie einzeln oder beide festlegen können.
  - Anzahl der gleichzeitig ausgeführten Instanzen beschränken auf:
  - Auf eine Instanz pro Benutzer beschränken

# Verwalten von Anwendungsordnern

Standardmäßig werden neue Anwendungen, die Sie Bereitstellungsgruppen hinzufügen, in einem Ordner mit dem Namen **Applications** abgelegt. Sie können bei der Erstellung der Bereitstellungsgruppe, beim Hinzufügen einer Anwendung oder zu einem anderen Zeitpunkt einen anderen Ordner angeben.

Gut zu wissen:

- Sie können den Ordner "Applications" nicht umbenennen oder löschen. Sie können aber alle Anwendungen in diesem Ordner in andere von Ihnen erstellte Ordner verschieben.
- Ein Ordnername darf 1-64 Zeichen enthalten. Leerstellen sind zugelassen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Ordner können bis zu fünffach verschachtelt werden.
- Ordner müssen keine Anwendungen enthalten, leere Ordner sind zugelassen.
- Ordner werden in Studio alphabetisch aufgelistet, es sei denn, Sie verschieben sie oder geben beim Erstellen einen anderen Speicherort an.
- Sie können mehr als einen Ordner mit dem gleichen Namen haben, sofern jeder einen anderen übergeordneten Ordner hat. Sie können mehr als eine Anwendung mit dem gleichen Namen haben, sofern jede in einem anderen Ordner ist.
- Zum Entfernen, Umbenennen und Löschen eines Ordners, der Anwendungen enthält, benötigen Sie für alle enthaltenen Anwendungen die Berechtigung zum Anzeigen von Anwendungen in Ordnern und die Berechtigung zum Bearbeiten der Anwendungseigenschaften.
- Die meisten der folgenden Verfahren umfassen Aktionen aus dem Bereich "Aktionen" in Studio. Alternativ können Sie Kontextmenüs oder Drag & Drop verwenden. Wenn Sie beispielsweise einen Ordner am falschen Speicherort erstellen oder ihn dorthin verschieben, können Sie ihn per Drag & Drop an den korrekten Speicherort ziehen.

Zum Verwalten von Anwendungsordnern wählen Sie im Studio-Navigationsbereich **Anwendungen**. Orientieren Sie sich an der nachfolgenden Liste.

- Zum Anzeigen aller Ordner (unter Ausschluss verschachtelter Ordner) klicken Sie oberhalb der Ordnerliste auf **Alle anzeigen**.
- Zum Erstellen eines (unverschachtelten) Ordners auf der höchsten Ebene wählen Sie den Anwendungsordner aus. Zum Erstellen des Ordners als Unterordner eines vorhandenen Ordners wählen Sie diesen Ordner aus. Wählen Sie dann im Aktionsbereich **Ordner erstellen**. Geben Sie einen Namen ein.
- Zum Verschieben eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner verschieben**. Sie können immer nur einen Ordner verschieben, es sei denn, der Ordner enthält Unterordner. Tipp: Die einfachste Möglichkeit zum Verschieben von Ordnern ist Drag & Drop.
- Zum Umbenennen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner umbenennen**. Geben Sie einen Namen ein.
- Zum Löschen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner löschen**. Beim Löschen eines Ordners, der Anwendungen und andere Ordner enthält, werden diese Objekte auch gelöscht. Beim Löschen einer Anwendung wird die Anwendungszuweisung aus der Bereitstellungsgruppe aber nicht aus der Maschine entfernt.
- Zum Verschieben von Anwendungen in einen Ordner wählen Sie eine oder mehrere Anwendungen. Wählen Sie dann im Aktionsbereich **Anwendung verschieben**. Wählen Sie den Ordner aus.

In den Assistenten zum Erstellen von Bereitstellungsgruppen und Anwendungsgruppen können Sie Anwendungen, die Sie hinzufügen, auf der Seite **Anwendung** auch in einem bestimmten Ordner oder einem neuen Ordner platzieren. Standardmäßig werden hinzugefügte Anwendungen im Ordner "Applications" abgelegt. Klicken Sie auf **Ändern**, um einen Ordner auszuwählen oder zu erstellen).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Zonen

Jul 08, 2016

In Bereitstellungen mit weit auseinanderliegenden Standorten in einem WAN kann es zu Latenz- und Zuverlässigkeitsproblemen kommen. Es gibt zwei Möglichkeiten, diesen Herausforderungen zu begegnen:

- Bereitstellen mehrerer Sites mit eigener SQL Server-Sitedatenbank:

  Diese Option empfiehlt sich für große Unternehmen. Mehrere Sites können einzeln verwaltet werden und erfordern alle eine eigene SQL Server-Sitedatenbank. Jede Site ist eine eigenständige XenApp-Bereitstellung.

- Konfigurieren mehrerer Zonen in einer einzelnen Site:

  Mit Zonen können Benutzer an entfernten Standorten eine Verbindung mit Ressourcen herstellen, ohne dass die Verbindungen durch große WAN-Segmente laufen müssen. Zonen gestatten eine effektive Siteverwaltung über eine einzelne Citrix Studio-Konsole, Citrix Director und die Sitedatenbank. Auf diese Weise können die Kosten für Bereitstellung, Personalbesetzung, Lizenzierung und Betrieb zusätzlicher Sites mit eigenen Datenbanken an entfernten Standorten gespart werden.

  Zonen können bei Bereitstellungen aller Größen nützlich sein. Mit Zonen können Sie Anwendungen und Desktops näher an den Benutzern ansiedeln und so die Leistung verbessern. Aus Redundanz- und Flexibilitätsgründen ist die Installation eines oder mehrerer Controller zonenlokal möglich, jedoch nicht erforderlich.

In diesem Artikel bezieht sich der Begriff "lokal" auf die jeweils behandelte Zone. "Ein VDA registriert sich bei einem lokalen Controller" bedeutet beispielsweise, dass sich der VDA bei einem Controller in der Zone registriert, in der der VDA ist.

Die Zonen in diesem Release ähneln denen in XenApp 6.5 und Vorversionen, sind mit ihnen jedoch nicht identisch. Beispielsweise gibt es in dieser Zonenimplementierung keine Datensammelpunkte. Alle Controller in einer Site kommunizieren mit einer Sitedatenbank in der primären Zone. Auch Failover und bevorzugte Zonen funktionieren in diesem Release anders.

# Zonentypen

Eine Site hat immer eine primäre Zone. Sie kann auch eine oder mehrere Satellitenzonen haben. Satellitenzonen können für die Notfallwiederherstellung, entfernte Datencenter, Zweigstellen, eine Cloud oder eine Availability Zone in einer Cloud verwendet werden.

**Primäre Zone**

Die primäre Zone hat den Standardnamen "Primär" und umfasst SQL Server-Sitedatenbank (sowie ggf. hoch verfügbare SQL Server-Computer), Studio, Director, Citrix StoreFront, Citrix Lizenzserver und NetScaler Gateway. Die Sitedatenbank muss immer in der primären Zone sein.

Die primäre Zone sollte aus Redundanzgründen außerdem mindestens zwei Controller enthalten und kann einen oder mehrere VDAs mit Anwendungen umfassen, die eng an die Datenbank und Infrastruktur gekoppelt sind.

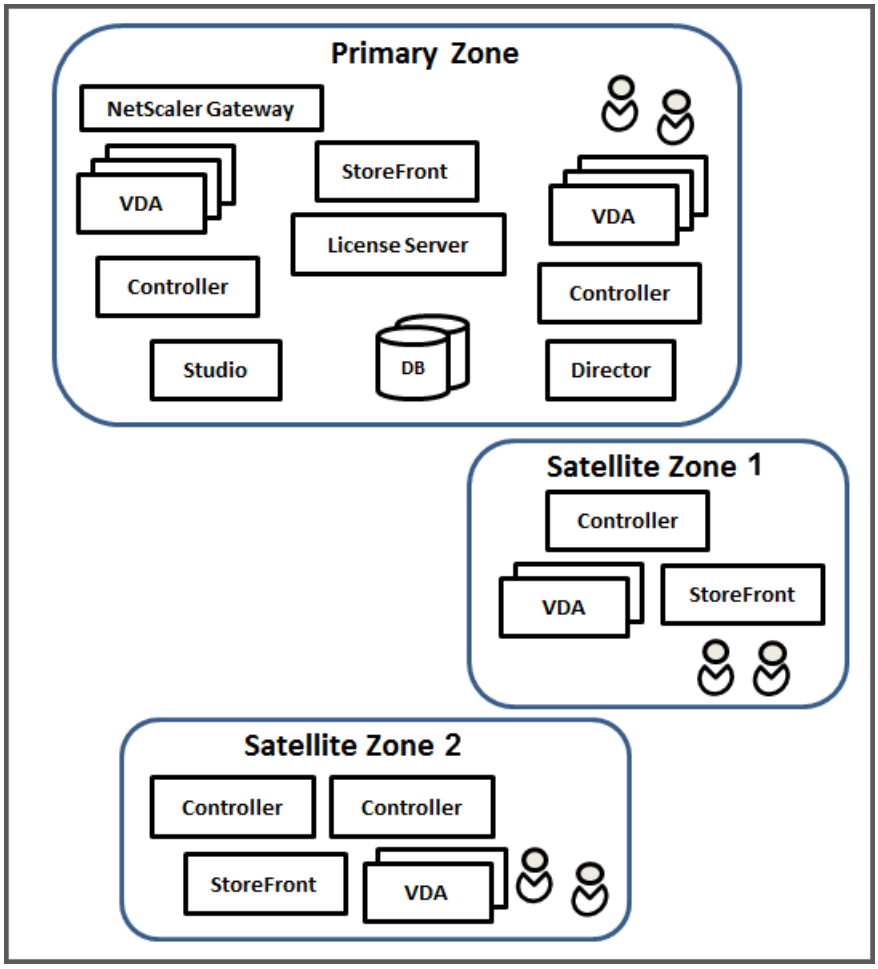
**Satellitenzonen**

Eine Satellitenzone enthält einen oder mehrere VDAs, Controller und StoreFront- sowie NetScaler Gateway-Server. Im Normalbetrieb kommunizieren Controller in einer Satellitenzone direkt mit der Datenbank in der primären Zone.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Satellitenzonen, insbesondere große, können auch einen Hypervisor für die Bereitstellung und/oder Speicherung von Maschinen enthalten. Beim Konfigurieren einer Satellitenzone können Sie dieser eine Hypervisor- oder Clouddienstverbindung zuweisen. Alle Maschinenkataloge, die diese Verbindung verwenden, müssen in der gleichen Zone sein.

Eine Site kann je nach Anforderungen und Umgebung verschiedene Arten von Satellitenzonen enthalten. Die folgende Abbildung zeigt eine primäre Zone und Beispiele von Satellitenzonen.




- Die primäre Zone enthält zwei Controller, Studio, Director, StoreFront, den Lizenzserver und die Sitedatenbank (sowie hoch verfügbare SQL Server-Bereitstellungen). Die primäre Zone enthält außerdem mehrere VDAs und ein NetScaler Gateway.
- Satellitenzone 1 – VDAs mit Controller

  Satellitenzone 1 enthält einen Controller, VDAs und einen StoreFront-Server. Die VDAs in dieser Satellitenzone registrieren sich bei dem lokalen Controller. Der lokale Controller kommuniziert mit der Sitedatenbank und dem Lizenzserver in der primären Zone.

  Wenn das WAN ausfällt, kann der Controller in der Satellitenzone dank Verbindungsleasing weiterhin Verbindungen mit VDAs in dieser Zone vermitteln. Eine solche Bereitstellung ist beispielsweise an Standorten nützlich, an denen Mitarbeiter über die lokale StoreFront-Site und den lokalen Controller auf ihre lokalen Ressourcen zugreifen, was möglich ist, selbst wenn die WAN-Verbindung zwischen dem Standort und dem Unternehmensnetzwerk ausfällt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Satellitenzone 2 – VDAs mit redundanten Controllern

  Satellitenzone 2 enthält zwei Controller, VDAs und einen StoreFront-Server. Dieser Zonentyp bietet die größte Resilienz bei gleichzeitigem Ausfall des WANs und eines lokalen Controllers.

# VDAs-Registrierung und Controllerfailover

Site mit primärer Zone und Satellitenzonen und VDAs, deren Version mindestens 7.7 ist:

- Ein VDA in der primären Zone registriert sich bei einem Controller in der primären Zone. Ein VDA in der primären Zone versucht nie eine Registrierung bei einem Controller in einer Satellitenzone.
- Ein VDA in einer Satellitenzone registriert sich bei einem lokalen Controller, sofern möglich. Dies ist der bevorzugte Controller. Sind keine lokalen Controller verfügbar (z. B. weil sie keine weiteren VDA-Registrierungen annehmen können oder weil sie ausgefallen sind), versucht der VDA die Registrierung bei einem Controller in der primären Zone. In diesem Fall bleibt der VDA in der primären Zone registriert, selbst wenn wieder ein Controller in der Satellitenzone verfügbar wird. Ein VDA in einer Satellitenzone versucht nie eine Registrierung bei einem Controller in einer anderen Satellitenzone.
- Wenn für die VDA-Ermittlung von Controllern die automatische Aktualisierung aktiviert ist und Sie bei der VDA-Installation eine Liste von Controlleradressen angegeben haben, wird aus dieser nach dem Zufallsprinzip ein Controller für die erste Registrierung ausgewählt, unabhängig davon, in welcher Zone der Controller residiert. Wenn die Maschine mit dem VDA neu gestartet wird, versucht dieser die Registrierung bei einem Controller in der lokalen Zone.
- Wenn ein Controller in einer Satellitenzone ausfällt, erfolgt, sofern möglich, ein Failover zu einem anderen lokalen Controller. Ist kein lokaler Controller verfügbar, erfolgt ein Failover auf einen Controller in der primären Zone.
- Wenn Sie einen Controller in eine Zone oder aus einer Zone verschieben und die automatische Aktualisierung aktiviert ist, erhalten die VDAs eine aktualisierte Liste der lokal und in der primären Zone angesiedelten Controller, anhand derer die Registrierung und die Annahme von Verbindungen erfolgt.
- Wenn Sie einen Maschinenkatalog in eine andere Zone verschieben, registrieren sich die VDAs in diesem Katalog bei Controllern in der Zone, in die Sie den Katalog verschoben haben. (Wenn Sie einen Katalog verschieben, verschieben Sie alle zugehörigen Hostverbindungen in die gleiche Zone.)
- Auf Controllern in der primären Zone werden Verbindungsleasingdaten für alle Zonen gespeichert. Auf Controllern in Satellitenzonen werden Verbindungsleasingdaten für die eigene Zone und die primäre Zone, jedoch nicht für die anderen Satellitenzonen gespeichert.

Sites mit VDAs vor Version 7.7:

- VDAs in einer Satellitenzone akzeptieren Anforderungen von Controllern in der lokalen Zone und der primären Zone. (VDAs ab Version 7.7 können Controlleranforderungen aus anderen Satellitenzonen akzeptieren.)
- VDAs in einer Satellitenzone registrieren sich nach dem Zufallsprinzip bei einem Controller in der lokalen Zone oder der primären Zone. Bei VDAs ab Version 7.7 ist die lokale die bevorzugte Zone.

# Überlegungen, Anforderungen und bewährte Methoden

- Sie können Controller, Maschinenkataloge und Hostverbindungen in einer Zone platzieren. Wenn ein Maschinenkatalog eine Hostverbindung verwendet, müssen Katalog und Verbindung in der gleichen Zone sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Beim Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe einer Produktionssite sind alle Elemente in der primären Zone. Sie können Satellitenzonen erst erstellen, wenn das anfängliche Setup abgeschlossen ist. Wenn Sie eine leere Site erstellen, enthält die primäre Zone zunächst nur einen Controller. Sie können Satellitenzonen vor oder nach dem Erstellen eines Maschinenkatalogs und einer Bereitstellungsgruppe erstellen.
- Beim Erstellen der ersten Satellitenzone mit einem oder mehreren Elementen verbleiben alle anderen Elemente der Site in der primären Zone.
- Die primäre Zone heißt standardmäßig "Primär". Sie können diesen Namen nach Wunsch ändern. Obwohl die primäre Zone in Studio als solche gekennzeichnet ist, empfiehlt sich die Verwendung eines Namens, anhand dessen sie sich leicht identifizieren lässt. Sie können die primäre Zone neu zuweisen, d. h. eine andere Zone als primäre Zone festlegen, die Sitedatenbank und alle hoch verfügbaren Server müssen jedoch immer in der primären Zone sein.
- Die Sitedatenbank muss immer in der primären Zone sein.
- Nach dem Erstellen von Zonen können Sie Elemente zwischen Zonen verschieben. Diese Flexibilität birgt jedoch das Risiko der Trennung von Elementen, die am besten in unmittelbarer Nähe zueinander funktionieren. Das Verschieben eines Maschinenkatalogs in eine andere Zone als die zugehörige Verbindung (Host), durch welche die Maschinen in dem Katalog erstellt werden, kann sich beispielsweise negativ auf die Leistung auswirken. Überlegen Sie daher vor dem Verschieben von Elementen zwischen Zonen, ob dies unerwünschte Auswirkungen haben könnte. Kataloge und zugehörige Hostverbindungen müssen in der gleichen Zone sein.
- Zur Erzielung der optimalen Leistung installieren Sie Studio und Director nur in der primären Zone. Wenn Sie eine zusätzliche Studio-Instanz in einer Satellitenzone installieren möchten, z. B. in einer Satellitenzone mit Controllern, die für ein Failover bei Ausfall der primären Zone verwendet wird, führen Sie Studio als lokal veröffentlichte Anwendung aus. Sie können auch von einer Satellitenzone auf Director zugreifen, da es eine Webanwendung ist.
- Idealerweise sollte NetScaler Gateway in einer Satellitenzone für Benutzerverbindungen aus anderen Zonen oder externen Orten verwendet werden, es kann jedoch auch für zoneninterne Verbindungen verwendet werden.

# Erstellen und Verwalten von Zonen

Ein Volladministrator kann alle Aufgaben der Zonenerstellung und -verwaltung ausführen. Sie können jedoch auch eine benutzerdefinierte Rolle zum Erstellen, Bearbeiten oder Löschen einer Zone erstellen. Das Verschieben von Elementen zwischen Zonen erfordert für die Zone selbst lediglich eine Leseberechtigung. Sie benötigen jedoch die Berechtigung zum Bearbeiten der Elemente, die Sie verschieben möchten. Zum Verschieben eines Maschinenkatalogs von einer Zone in eine andere brauchen Sie beispielsweise die Berechtigung zum Bearbeiten des Maschinenkatalogs. Weitere Informationen finden Sie im Artikel zur delegierten Administration.

**Verwendung von Provisioning Services:** Die Provisioning Services Console in diesem Release erkennt keine Zonen. Citrix empfiehlt daher die Verwendung von Studio zum Erstellen von Maschinenkatalogen, die Sie in Satellitenzonen platzieren möchten. Verwenden Sie den Assistenten in Studio zum Erstellen des Katalogs und geben Sie die richtige Satellitenzone an. Verwenden Sie dann die Provisioning Services Console zum Bereitstellen von Maschinen in diesem Katalog. Wenn Sie den Katalog mit dem Provisioning Services-Assistenten erstellen, wird er in die primäre Zone platziert und muss anschließend mit Studio in die Satellitenzone verschoben werden.

## Erstellen von Zonen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie im Aktionsbereich **Zone erstellen**.
3. Geben Sie einen Namen für die Zone und optional eine Beschreibung ein. Der Name muss innerhalb der Site eindeutig sein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Wählen Sie die Elemente, die Sie in der neuen Zone platzieren möchten. Sie können die Liste der verfügbaren Elemente filtern oder durchsuchen. Sie können auch eine leere Zone erstellen. Wählen Sie hierfür einfach keine Elemente aus.
5. Klicken Sie auf **Save**.

Alternativ zu dieser Methode können Sie in Studio ein oder mehrere Elemente und im Aktionsbereich dann **Zone erstellen** wählen.

### Ändern des Namen oder der Beschreibung einer Zone

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie eine Zone und dann im Aktionsbereich **Zone bearbeiten**.
3. Ändern Sie den Zonennamen und/oder die Beschreibung. Wenn Sie den Namen der primären Zone ändern, stellen Sie sicher, dass sie weiterhin eindeutig als primäre Zone identifiziert werden kann.
4. Klicken Sie auf **OK** oder **Übernehmen**.

### Verschieben von Elementen zwischen Zonen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie mindestens ein Element aus.
3. Ziehen Sie das Element in die Zielzone oder wählen Sie im Aktionsbereich **Elemente verschieben** und geben Sie dann die gewünschte Zielzone an.

Durch eine Meldung mit einer Liste der ausgewählten Elemente werden Sie aufgefordert, das Verschieben zu bestätigen.

**Nicht vergessen:** Wenn ein Maschinenkatalog eine Hostverbindung zu einem Hypervisor oder Clouddienst verwendet, müssen Katalog und Verbindung in der gleichen Zone sein. Andernfalls kann die Leistung leiden. Wenn Sie eines dieser Elemente verschieben, verschieben Sie auch das andere.

### Löschen von Zonen

Eine Zone muss leer sein, damit sie gelöscht werden kann. Die primäre Zone kann nicht gelöscht werden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie eine Zone aus.
3. Wählen Sie im Aktionsbereich **Zone löschen**. Wenn die Zone nicht leer ist, werden Sie aufgefordert, die Zone auszuwählen, in die die enthaltenen Elemente verschoben werden sollen.
4. Bestätigen Sie die Löschung.

### Andere Aktionen, die eine Angabe von Zonen erfordern

In Sites mit mindestens einer Satellitenzone können Sie beim Hinzufügen einer Hostverbindung und beim Erstellen eines Maschinenkatalogs (nach Erstellen der Site) eine Zone für dieses Element angeben.

In den meisten Fällen ist die primäre Zone die Standardeinstellung. Wenn Sie einen Maschinenkatalog mit den Maschinenerstellungsdiensten erstellen, wird die für die Hostverbindung konfigurierte Zone automatisch ausgewählt.

Enthält die Site keine Satellitenzonen, wird die primäre Zone ausgewählt und die Option zur Auswahl der Zone wird nicht angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verbindungen und Ressourcen

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


- Einführung
- Informationen zu Verbindungstypen
- Hostspeicher
- Erstellen von Ressourcen und einer Verbindung
- Erstellen von Ressourcen und einer Verbindung aus einer vorhandenen Verbindung
- Bearbeiten von Verbindungseinstellungen
- Aktivieren und Deaktivieren des Wartungsmodus für eine Verbindung
- Löschen einer Verbindung
- Umbenennen oder Testen einer Verbindung
- Anzeigen von Maschinendetails für eine Verbindung
- Verwalten von Maschinen einer Verbindung
- Bearbeiten des Speichers
- Löschen, Umbenennen oder Testen von Ressourcen
- Verwenden von IntelliCache für XenServer-Verbindungen
- Verbindungstimer


# Einführung

Sie können die erste Verbindung mit Hosting-Ressourcen erstellen, wenn Sie eine Site erstellen. Später können Sie die Verbindung ändern und weitere Verbindungen erstellen. Beim Konfigurieren einer Verbindung wählen Sie den Typ der Verbindung aus der Liste unterstützter Hypervisors und Clouddienste aus. Der von Ihnen ausgewählte Speicher und das Netzwerk sind die Ressourcen der Verbindung.

Lesezugriffadministratoren können die Verbindung und Ressourcendetails anzeigen. Sie müssen Volladministrator sein, um Verwaltungsaufgaben an Verbindungen und Ressourcen durchzuführen. Weitere Informationen finden Sie im Artikel zur delegierten Administration.

## Informationen zu Verbindungstypen

Mit den unterstützten Virtualisierungsplattformen können Sie Maschinen in der XenApp- oder XenDesktop-Umgebung hosten und verwalten. In dem Artikel über die Systemanforderungen werden die unterstützten Typen aufgeführt. Sie können mit den unterstützten Cloudbereitstellungslösungen Produktkomponenten hosten und virtuelle Maschinen bereitstellen. Mit diesen Lösungen werden Computing-Ressourcen gepoolt, um öffentliche oder private Infrastructure-as-a-Service (IaaS)-Clouds sowie Hybrid-IaaS-Clouds zu erstellen.

Weitere Informationen finden Sie in den folgenden Informationsquellen:

VMware

- Artikel über VMware-Virtualisierungsumgebungen
- VMware-Produktdokumentation


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Hyper-V

- Artikel über Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Microsoft Azure

- Artikel über Microsoft Azure-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Amazon Web Services (AWS)

- Citrix XenDesktop auf AWS.
- AWS-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS oder CloudPlatform exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Availability Zone, VPC-Namen, Subnetzadressen, Domänenname, Namen der Sicherheitsgruppen und Anmeldeinformationen angeben.
- Die für das AWS-Rootkonto von der AWS-Konsole abgerufene Anmeldeinformationsdatei hat nicht das gleiche Format wie die Anmeldeinformationsdateien, die für Standard-AWS-Benutzer heruntergeladen werden. Deshalb kann diese Datei von Studio nicht zum Ausfüllen der Felder "API-Schlüssel" und "Geheimer Schlüssel" verwendet werden. Verwenden Sie AWS IAM-Anmeldeinformationsdateien.

Citrix CloudPlatform

- Citrix CloudPlatform-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus CloudPlatform exportieren und anschließend in Studio importieren.

Citrix XenServer

- Citrix XenServer-Dokumentation
- Beim Erstellen einer Verbindung müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.
- Citrix empfiehlt die Verwendung von HTTPS zur Sicherung der Kommunikation mit XenServer. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte SSL-Zertifikat ersetzen (siehe CTX128656).
- Sie können hohe Verfügbarkeit konfigurieren, wenn diese auf XenServer aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über "Server mit hoher Verfügbarkeit bearbeiten") auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.
- Sie können einen GPU-Typ und eine GPU-Gruppe oder Passthrough auswählen, wenn der XenServer vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

Nutanix Acropolis

- Artikel über Nutanix-Virtualisierungsumgebungen
- Nutanix-Dokumentation.

# Host storage


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Beim Provisioning von Maschinen werden die Daten nach Typ klassifiziert:

- Betriebssystemdaten (OS-Daten), einschließlich Masterimages.
- Temporäre Daten, einschließlich aller nicht persistenten Daten, die auf mit MSC bereitgestellten Maschinen geschrieben werden, Windows-Seitendateien, Benutzerprofildaten und alle Daten, die mit ShareFile synchronisiert werden. Diese Daten werden beim Neustart einer Maschine verworfen.
- Persönliche Daten, die auf persönlichen vDisks gespeichert werden.

Durch die Bereitstellung von separatem Speicher für die einzelnen Datentypen können Sie auf Speichergeräten die Last reduzieren und die IOPS-Leistung verbessern und so den größten Nutzen aus den verfügbaren Ressourcen des Hosts ziehen. Außerdem kann so der entsprechende Speicher für die verschiedenen Datentypen verwendet werden, denn Persistenz und Resilienz ist für einige Daten wichtiger als für andere.

Speicher kann freigegeben sein (zentraler Speicher, der separat von den Hosts ist, aber von allen Hosts verwendet wird) oder lokal auf einem Hypervisor bereitgestellt werden. Ein zentraler freigegebener Speicher kann beispielsweise aus einem oder mehreren geclusterten Windows Server 2012-Speichervolumes (mit oder ohne angeschlossenem Speicher) oder dem Gerät eines Speicheranbieters bestehen. Der zentrale Speicher bietet möglicherweise auch eigene Optimierungen, wie Steuerungspfade für Hypervisorspeicher und direkter Zugriff über Partner-Plug-Ins.

Durch das lokale Speichern temporärer Daten muss für den Zugriff auf freigegebenen Speicher nicht das Netzwerk passiert werden. Dadurch wird die Last (IOPS) auf dem freigegebenen Speichergerät reduziert. Freigegebener Speicher kann kostspieliger sein, daher können durch das lokale Speichern von Daten die Ausgaben gesenkt werden. Diese Vorteile müssen gegen die Verfügbarkeit von genügend Speicher auf den Hypervisorservern abgewogen werden.

Beim Erstellen einer Verbindung müssen Sie eine von zwei Speicherverwaltungsmethoden auswählen: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

**Hinweis:** Wenn Sie auf XenServer-Hosts lokalen Speicher für die temporäre Datenspeicherung verwenden, stellen Sie sicher, dass jeder Speicherort im Pool einen eindeutigen Namen hat. (Sie ändern einen Namen in XenCenter, indem Sie mit der rechten Maustaste auf den Speicher klicken und die Nameneigenschaft bearbeiten.

### Für Hypervisors freigegebener Speicher

Bei für Hypervisors freigegebenem Speicher werden Daten, die länger erhalten bleiben sollen, zentral gespeichert und bieten zentrale Backup- und Verwaltungsmöglichkeiten. Dieser Speicher umfasst die Betriebssystemdatenträger und die persönlichen vDisk-Datenträger.

Bei dieser Methode können Sie wählen, ob Sie lokalen Speicher (auf Servern im gleichen Hypervisorpool) für temporäre Daten verwenden, die nicht so viel Persistenz oder Resilienz erfordern wie die Daten im freigegebenen Speicher. Dies wird als *temporärer Datencache* bezeichnet. Die lokale Festplatte reduziert den Datenverkehr zum Hauptbetriebssystemspeicher. Dieser Datenträger wird nach dem Neustart einer Maschine gelöscht. Auf den Datenträger wird über einen Write-through-Speichercache zugegriffen. Wenn Sie lokalen Speicher für temporäre Daten verwenden, ist der bereitgestellte VDA an einen bestimmten Hypervisorhost gebunden. Wenn der Host ausfällt, kann die VM nicht gestartet werden.

**Ausnahme**: Wenn Sie geclusterte Speichervolumes (CSV) verwenden, erlaubt Microsoft System Center Virtual Machine Manager nicht, dass temporäre Datenträgercaches auf dem lokalen Speicher erstellt werden.

Wenn Sie beim Erstellen einer Verbindung die Option für die lokale Speicherung der temporären Daten aktivieren, können Sie benutzerdefinierte Werte für die Größe des Cachedatenträgers und des Speichers jeder VM aktivieren und konfigurieren, wenn Sie einen Maschinenkatalog erstellen, der diese Verbindung verwendet. Die Standardwerte sind jedoch auf den


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verbindungstyp zugeschnitten und in den meisten Fällen ausreichend. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Der Hypervisor kann auch Optimierungstechnologien über lokales Lese-Caching der Datenträgerimages bieten; XenServer bietet beispielsweise IntelliCache. Dies kann auch den Netzwerkdatenverkehr zum zentralen Speicher reduzieren.

### Lokaler Speicher auf dem Hypervisor

Bei der Methode mit lokalem Speicher auf dem Hypervisor werden Daten lokal auf dem Hypervisor gespeichert. Mit dieser Methode werden Masterimages und andere Betriebssystemdaten an alle Hypervisors in der Site übermittelt, sowohl bei der anfänglichen Maschinenerstellung als auch bei zukünftigen Imageupdates. Dies führt zu intensivem Datenverkehr auf dem Verwaltungsnetzwerk. Imageübertragungen sind zeitaufwändig und die Images werden jedem Host zu einem anderen Zeitpunkt zur Verfügung gestellt.

Bei Auswahl dieser Methode können Sie wählen, ob Sie freigegebenen Speicher für persönliche vDisks verwenden, um Resilienz und Unterstützung für Backup- und Notfallwiederherstellungssysteme bieten.

# Erstellen von Ressourcen und einer Verbindung

Sie können die erste Verbindung beim Erstellen der Site erstellen. Der Assistent für die Siteerstellung enthält die nachfolgend beschriebenen Seiten für Verbindungen: Verbindung, Speicherverwaltung, Speicherauswahl und Netzwerk.

Wenn Sie eine Verbindung erstellen, nachdem Sie die Site erstellt haben, beginnen Sie mit Schritt 1 (siehe unten).

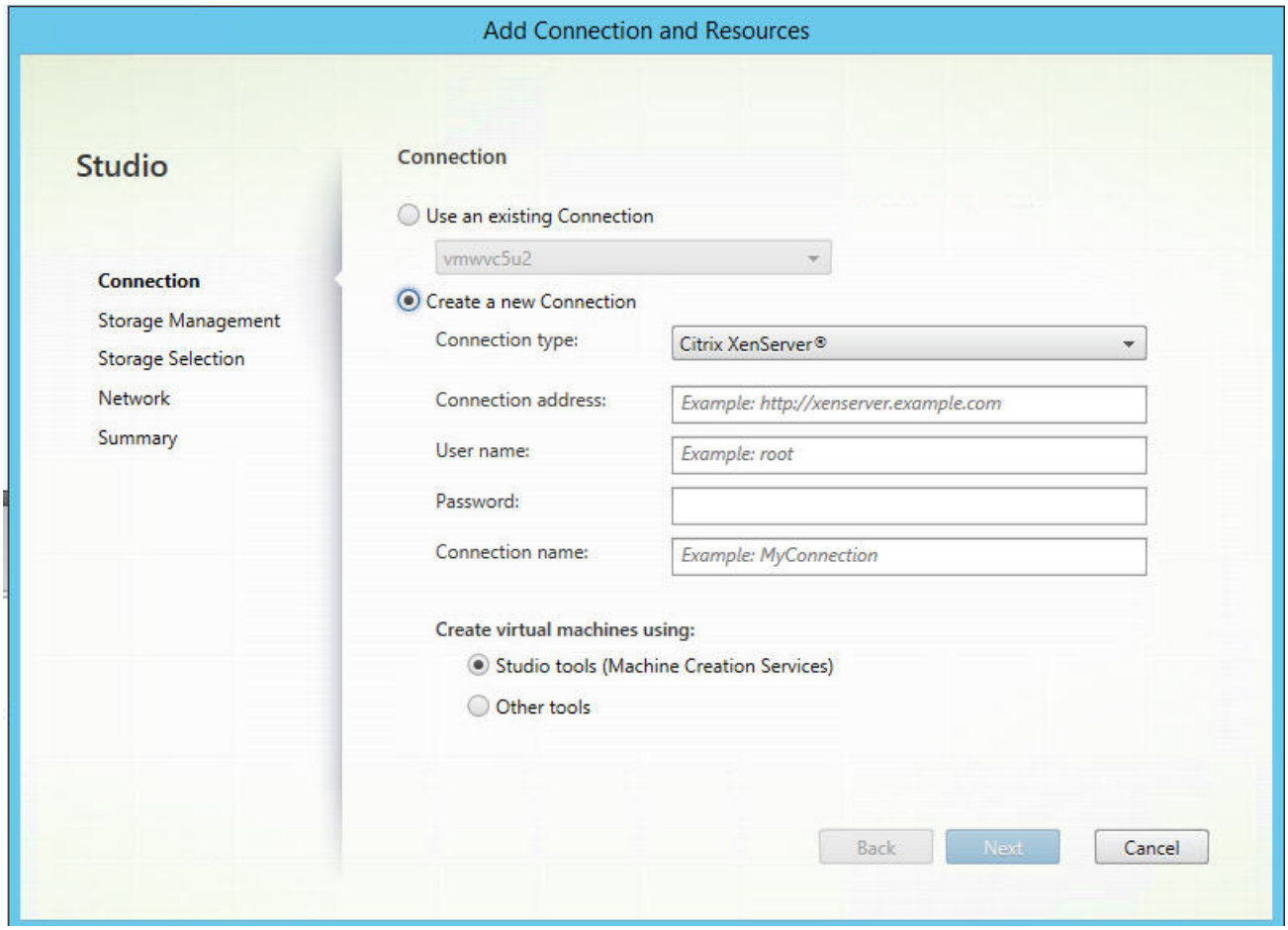
Wenn Sie eine Verbindung basierend auf der Hostkonfiguration einer bestehenden Verbindung erstellen, verwenden Sie dieses Verfahren.

**Wichtig:** Die Hostressourcen (Speicher und Netzwerk) müssen verfügbar sein, bevor Sie eine Verbindung zu erstellen.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie im Aktionsbereich **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie **Neue Verbindung erstellen**.
4. Der Assistent führt Sie durch die folgenden Seiten (der Seiteninhalt hängt vom ausgewählten Verbindungstyp ab). Nehmen Sie auf den Seiten die erforderlichen Angaben vor und klicken Sie auf **Weiter**, bis die Seite "Zusammenfassung" angezeigt wird.

### Verbindung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

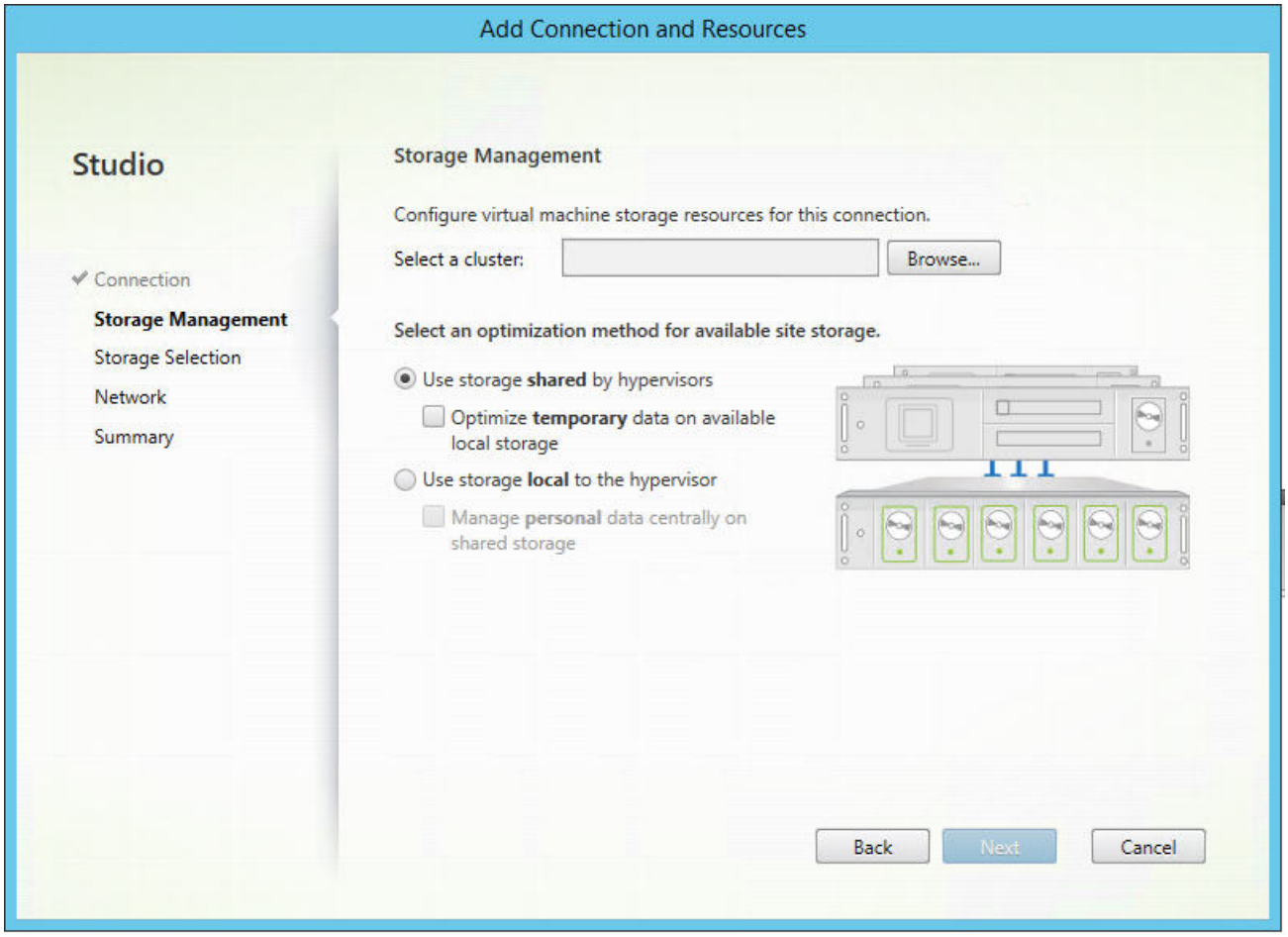



Treffen Sie auf der Seite **Verbindung** folgende Auswahl:

- Wählen Sie im Feld **Verbindungstyp** den Hypervisor oder Cloud-Dienst, den Sie verwenden.
- Die Felder für Verbindungsadresse und Anmeldeinformationen sind je nach ausgewähltem Verbindungstyp unterschiedlich. Geben Sie die angeforderten Informationen ein.
- Geben Sie einen Verbindungsnamen ein. Dieser Name wird in Studio angezeigt.
- Wählen Sie das Tool, mit dem Sie virtuelle Maschinen erstellen: Studio-Tools (z. B. Maschinenerstellungsdienste (MCS) oder Provisioning Services) oder andere Tools.

## Speicherverwaltung


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Informationen zur Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keine Clusternamen.

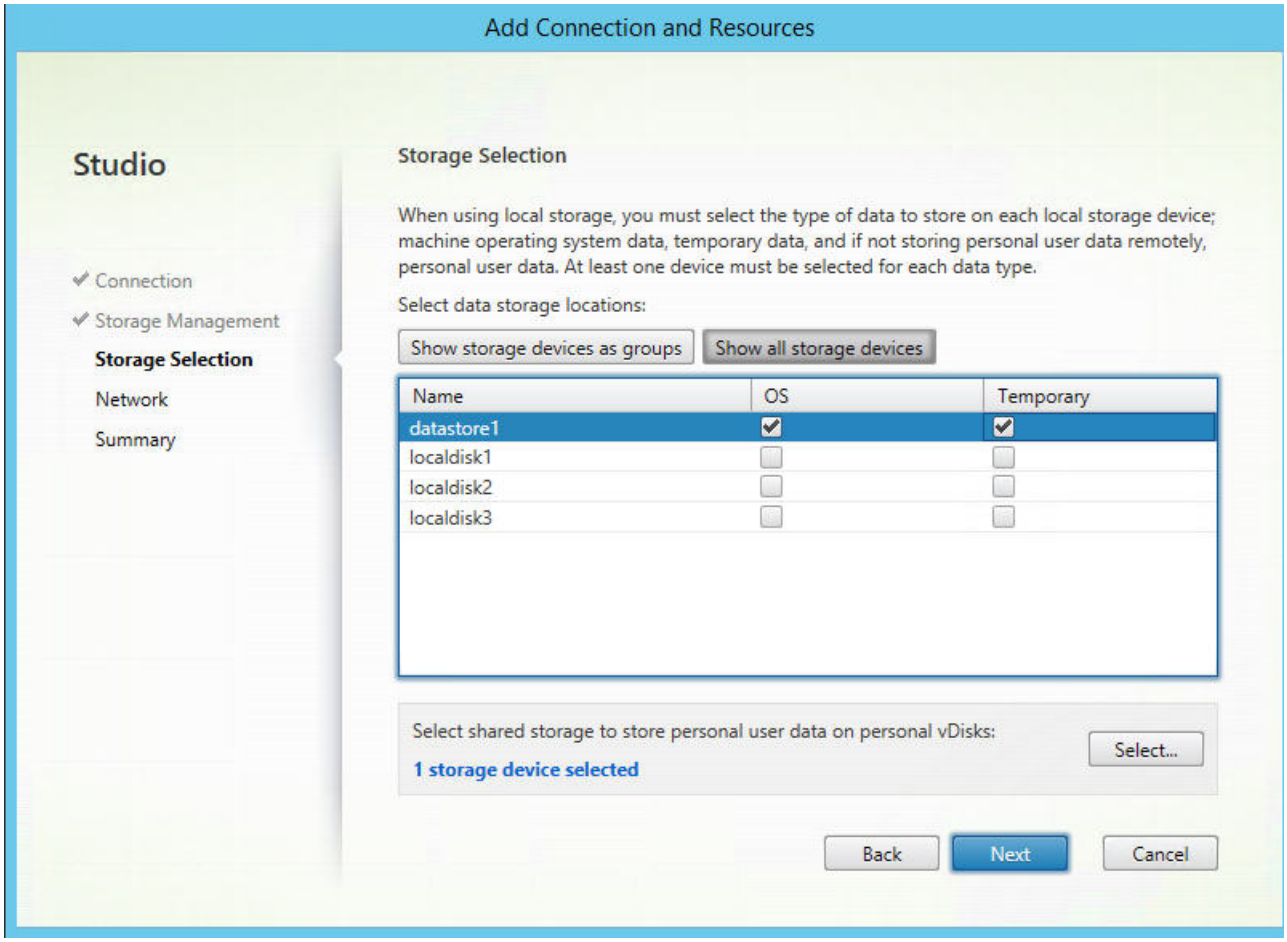
Wählen Sie eine Speicherverwaltungsmethode: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

- Wenn Sie für Hypervisors freigegebenen Speicher wählen, geben Sie an, ob temporäre Daten im verfügbaren lokalen Speicher gespeichert werden sollen. (Sie können nicht standardmäßige temporäre Speichergrößen in den Maschinenkatalogen angeben, die diese Verbindung verwenden.) **Ausnahme:** Wenn Sie geclusterte Speichervolumes (CSV) verwenden, erlaubt Microsoft System Center Virtual Machine Manager nicht, dass temporäre Datenträgercaches auf dem lokalen Speicher erstellt werden, daher schlägt das Konfigurieren des Speicherverwaltungssetups in Studio fehl.
- Wenn Sie lokalen Speicher auf dem Hypervisor wählen, geben Sie an, ob Sie persönliche Daten (persönliche vDisks) im freigegebenen Speicher verwalten möchten.

Wenn Sie freigegebenen Speicher auf einem XenServer-Hypervisor verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Weitere Informationen finden Sie unter Verwenden von IntelliCache für XenServer-Verbindungen.

## Speicherauswahl


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

Wählen Sie mindestens ein Hostspeichergerät für jeden verfügbaren Datentyp. Die auf der vorherigen Seite ausgewählte Speicherverwaltungsmethode bestimmt, welche Datentypen Sie auf dieser Seite auswählen können. Wählen Sie mindestens ein Speichergerät für jeden unterstützten Datentyp, bevor Sie mit der nächsten Seite im Assistenten fortfahren.

Der untere Teil der Seite **Speicherauswahl** enthält weitere Konfigurationsoptionen, wenn Sie eine der folgenden Optionen auf der vorherigen Seite ausgewählt haben.

- Wenn Sie für Hypervisors freigegebenen Speicher und das Kontrollkästchen **Temporäre Daten in verfügbarem lokalem Speicher optimieren** ausgewählt haben, können Sie wählen, welche lokalen Speichergeräte (im gleichen Hypervisorpool) für temporäre Daten verwendet werden.
- Wenn Sie lokalen Speicher auf dem Hypervisor und das Kontrollkästchen **Persönliche Daten zentral im freigegebenen Speicher verwalten** ausgewählt haben, können Sie auswählen, welche freigegebenen Geräte für persönliche (PvD) Daten genutzt werden.

Die Anzahl der zurzeit ausgewählten Speichergeräte wird angezeigt (siehe Abbildung oben: "1 Speichergerät ausgewählt"). Wenn Sie mit dem Mauszeiger darauf zeigen, werden die Namen der ausgewählten Geräte angezeigt, es sei denn, es sind keine Geräte konfiguriert.

1. Klicken Sie auf **Auswählen**, um die zu verwendenden Speichergeräte zu ändern.
2. Aktivieren oder deaktivieren Sie die Kontrollkästchen der entsprechenden Speichergeräte im Dialogfeld **Speicher auswählen** und klicken Sie dann auf **OK**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Netzwerk

Geben Sie einen Namen für die Ressourcen ein. Dieser Name wird in Studio angezeigt, um das Speichergerät und die der Verbindung zugeordnete Netzwerkkombination zu identifizieren.

Wählen Sie mindestens ein Netzwerk für die VMs aus.

### Zusammenfassung

Überprüfen Sie Ihre Auswahl. Wenn Sie Änderungen vornehmen möchten, kehren Sie zu den vorherigen Seiten des Assistenten zurück. Wenn Sie die Überprüfung abgeschlossen haben, klicken Sie auf **Fertig stellen**.

**Wichtig**: Wenn Sie temporäre Daten lokal speichern, können Sie benutzerdefinierte Werte für den temporären Datenspeicher konfigurieren, wenn Sie den Maschinenkatalog mit den Maschinen für diese Verbindung erstellen. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

# Erstellen von Ressourcen und einer Verbindung aus einer vorhandenen Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie im Aktionsbereich **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie **Vorhandene Verbindung verwenden** und dann die gewünschte Verbindung.
4. Der Assistent führt Sie durch die Seiten, die unter Erstellen von Ressourcen und einer Verbindung beschrieben wurden.

# Bearbeiten von Verbindungseinstellungen

Verwenden Sie diese Vorgehensweise nicht, um eine Verbindung umzubenennen oder eine neue Verbindung zu erstellen. Dafür sind andere Schritte erforderlich. Ändern Sie die Adresse nur, wenn die aktuelle Hostmaschine eine neue Adresse hat. Durch die Eingabe der Adresse einer anderen Maschine werden die Maschinenkataloge der Verbindung unbrauchbar.

Sie können die GPU-Einstellungen für eine Verbindung nicht ändern, da Maschinenkataloge, die auf diese Ressource zugreifen, ein entsprechendes GPU-spezifisches Masterimage verwenden müssen. Erstellen Sie eine neue Verbindung.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung bearbeiten**.
3. Folgen Sie den Anweisungen unten bei der Auswahl der Einstellungen zum Bearbeiten einer Verbindung.
4. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Seite **Verbindungseigenschaften**:

- Zum Ändern der Verbindungsadresse und Anmeldeinformationen wählen Sie **Einstellungen bearbeiten** und geben die neuen Informationen ein.
- Zum Festlegen der Server mit hoher Verfügbarkeit für eine XenServer-Verbindung wählen Sie **Server mit hoher Verfügbarkeit bearbeiten**. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seite **Erweitert**:

Für eine Wake-On-LAN-Verbindung unter Microsoft System Center Configuration Manager, die mit Remote-PC-Zugriff verwendet wird, geben Sie ConfigMgr Wake Proxy, Magic Packets und Paketübertragungsinformationen an.

Über die Einstellungen für den Einschränkungsschwellenwert können Sie eine maximale Anzahl von Energieaktionen für eine Verbindung festlegen. Diese Einstellungen können nützlich sein, wenn durch die Energieverwaltungseinstellungen der gleichzeitige Start zu vieler oder zu weniger Maschinen zugelassen wird. Für jeden Verbindungstyp gibt es bestimmte Standardwerte, die in den meisten Fällen geeignet sind und in der Regel nicht geändert werden sollten.

Über **Gleichzeitige Aktionen (alle Typen)** und **Gleichzeitige Updates für Personal vDisk-Inventar** wird Folgendes festgelegt: die maximale absolute Zahl Aktionen/Updates, die gleichzeitig an dieser Verbindung auftreten dürfen, und den maximalen Prozentsatz aller Maschinen, die diese Verbindung verwenden. Sie müssen beide Werte angeben, angewendet wird der geringere der Werte.

Beispiel: Wird in einer Bereitstellung mit 34 Maschinen die Einstellung **Gleichzeitige Aktionen (alle Typen)** auf einen absoluten Wert von 10 und einen Prozentsatz von 10 festgelegt, wird als tatsächliches Limit 3 angewendet (d. h. 10 Prozent von 34 auf die nächste Ganzzahl gerundet – ein kleinerer Wert als die absolute Zahl von 10 Maschinen).

Der Wert für **Höchstanzahl neue Aktionen pro Minute** ist eine absolute Zahl, kein Prozentwert.

**Hinweis:** Geben Sie die Informationen im Feld **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix ein.

# Aktivieren und Deaktivieren des Wartungsmodus für eine Verbindung

Wenn Sie den Wartungsmodus für eine Verbindung aktivieren, können keine neuen Energieaktionen auf in dieser Verbindung gespeicherten Maschinen stattfinden. Benutzer können keine Verbindung mit einer Maschine herstellen, wenn sie im Wartungsmodus ist. Wenn Benutzer bereits verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung aus. Zum Aktivieren des Wartungsmodus wählen Sie im Aktionsbereich **Wartungsmodus einschalten**. Zum Deaktivieren des Wartungsmodus wählen Sie **Wartungsmodus ausschalten**.

Sie können den Wartungsmodus auch für einzelne Maschinen ein- und ausschalten. Darüber hinaus können Sie den Wartungsmodus auch für Maschinen in Maschinenkatalogen und Bereitstellungsgruppen aktivieren oder deaktivieren.

# Löschen einer Verbindung

**Achtung:** Das Löschen einer Verbindung kann zur Folge haben, dass eine große Zahl von Maschinen gelöscht wird, Datenverlust eingeschlossen. Stellen Sie sicher, dass die Benutzerdaten auf den betroffenen Maschinen gesichert wurden oder nicht mehr benötigt werden.

Vor dem Löschen einer Verbindung müssen Sie Folgendes sicherstellen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Alle Benutzer sind von den in dieser Verbindung gespeicherten Maschinen abgemeldet.
- Es werden keine getrennten Benutzersitzungen ausgeführt.
- Der Wartungsmodus wird für gepoolte und dedizierte Maschinen aktiviert.
- Alle Maschinen in den von der Verbindung verwendeten Maschinenkatalogen sind ausgeschaltet.

Ein Maschinenkatalog kann nicht mehr verwendet werden, wenn Sie eine Verbindung löschen, auf die dieser Katalog verweist. Verweist ein Katalog auf diese Verbindung, haben Sie die Option zum Löschen des Katalogs. Stellen Sie vor dem Löschen eines Katalogs sicher, dass er nicht von anderen Verbindungen verwendet wird.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung löschen**.
3. Wenn für die Verbindung Maschinen gespeichert sind, werden Sie gefragt, ob die Maschinen gelöscht werden sollen. Wenn dies der Fall ist, geben Sie an, was mit dem zugewiesenen Active Directory-Computerkonten passieren soll.

# Umbenennen oder Testen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung umbenennen** oder **Verbindung testen**.

# Anzeigen von Maschinendetails für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Maschinen anzeigen**.

Im oberen Bereich werden die Maschinen angezeigt, auf die über die Verbindung zugegriffen wird. Wählen Sie eine Maschine aus, um die Details im unteren Bereich anzuzeigen. Für geöffnete Sitzungen werden auch Sitzungsdetails angezeigt.

Sie können das Suchfeature verwenden, um Maschinen schnell aufzufinden. Wählen Sie entweder eine gespeicherte Suche aus der Liste im oberen Bereich des Bildschirms aus oder erstellen Sie eine neue Suche. Sie können nach dem Maschinennamen suchen, indem Sie den ganzen Namen oder einen Teil des Namens eingeben. Alternativ können Sie auch einen Ausdruck für eine erweiterte Suche erstellen. Klicken Sie auf dieErweiterungsschaltfläche, um einen Ausdruck zu erstellen, und wählen Sie dann aus den angezeigten Listen Eigenschaften und Operatoren aus.

# Verwalten von Maschinen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie eine Verbindung und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine der folgenden Aktionen im Aktionsbereich. Abhängig vom Maschinenzustand und dem Verbindungshosttyp sind einige Aktionen möglicherweise nicht verfügbar.

- **Starten**: Die Maschine wird gestartet, wenn sie ausgeschaltet oder angehalten ist.
- **Anhalten**: Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
- **Herunterfahren**: Das Betriebssystem wird aufgefordert, herunterzufahren.
- **Herunterfahren erzwingen**: Die Maschine wird zwingend abgeschaltet und die Liste der Maschinen wird aktualisiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Neu starten**: Das Betriebssystem wird heruntergefahren und die Maschine wird neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt der Desktop im aktuellen Zustand.
- **Wartungsmodus aktivieren:** Die Verbindungen zu einer Maschine werden vorübergehend unterbrochen. Benutzer können keine Verbindung mit einer Maschine in diesem Zustand herstellen. Wenn Benutzer verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden. Sie können den Wartungsmodus auch für alle Maschinen aktivieren bzw. deaktivieren, auf die über eine Verbindung zugegriffen wird (siehe oben).
- **Aus Bereitstellungsgruppe entfernen**: Beim Entfernen einer Maschine aus einer Bereitstellungsgruppe wird sie nicht aus dem von der Bereitstellungsgruppe verwendeten Maschinenkatalog gelöscht. Sie können eine Maschine nur entfernen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine entfernen.
- **Löschen**: Wenn Sie eine Maschine löschen, können Benutzer nicht mehr darauf zugreifen und die Maschine wird aus dem Maschinenkatalog gelöscht. Stellen Sie vor dem Löschen einer Maschine sicher, dass alle Benutzerdaten gesichert wurden oder nicht mehr benötigt werden. Sie können eine Maschine nur löschen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine löschen.

Bei Aktionen, bei denen eine Maschine heruntergefahren wird, wird diese ausgeschaltet, wenn das Herunterfahren nicht innerhalb von 10 Minuten erfolgt. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

# Bearbeiten des Speichers

Sie können den Status der Server anzeigen, auf denen das Betriebssystem sowie temporäre und persönliche Daten (PvD) für VMs gespeichert werden, die eine Verbindung verwenden. Sie können auch festlegen, welche Server für die Speicherung der jeweiligen Datentypen verwendet werden.

1. Wählen Sie im Studio-Navigationsbereich "Konfiguration > Hosting".
2. Wählen Sie die Verbindung und dann im Aktionsbereich "Speicher bearbeiten".
3. Wählen Sie im linken Bereich den Datentyp: Betriebssystem, persönliche vDisk oder temporär.
4. Aktivieren oder deaktivieren Sie für den ausgewählten Datentyp das Kontrollkästchen für mindestens ein Speichergerät.
5. Klicken Sie auf "OK".

Jedes Speichergerät in der Liste enthält den Namen und Speicherstatus. Gültige Speicherstatuswerte sind Folgende:

- **Wird verwendet**: Der Speicher wird zum Erstellen neuer Maschinen verwendet.
- **Abgelöst**: Der Speicher wird nur für vorhandene Maschinen verwendet. Diesem Speicher werden keine neuen Maschinen hinzugefügt.
- **Nicht verwendet**: Der Speicher wird nicht zum Erstellen von Maschinen verwendet.

Wenn Sie das Kontrollkästchen eines Geräts deaktivieren, dessen Status **Wird verwendet** ist, ändert sich der Status in **Abgelöst**. Vorhandene Maschinen verwenden das Speichergerät weiterhin (und können Daten darauf schreiben), daher kann der Speicher voll werden, selbst wenn er nicht mehr zum Erstellen neuer Maschinen verwendet wird.

# Löschen, Umbenennen oder Testen von Ressourcen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie die Ressource aus und wählen Sie dann den entsprechenden Eintrag im Aktionsbereich: **Ressourcen löschen**, **Ressourcen umbenennen** oder **Ressourcen testen**.

# Verwenden von IntelliCache für XenServer-Verbindungen

Durch den Einsatz von IntelliCache werden gehostete VDI-Bereitstellungen kostengünstiger, da eine Kombination aus freigegebenem und lokalem Speicher verwendet werden kann. Dies verbessert die Leistung und reduziert den Datenverkehr im Netzwerk. Das Masterimage aus dem freigegebenen Speicher wird im lokalen Speicher zwischengespeichert, wodurch die Anzahl der Lesevorgänge im freigegebenen Speicher reduziert wird. Bei gemeinsam genutzten Desktops werden Schreibvorgänge auf den differenzierenden Festplatten in den lokalen Speicher auf dem Host und nicht in den gemeinsam genutzten Speicher geschrieben.

- Der freigegebene Speicher muss NFS sein, wenn Sie IntelliCache verwenden.
- Citrix empfiehlt die Verwendung eines lokalen Speichergeräts mit hoher Leistung, um eine schnellstmögliche Datenübertragung zu gewährleisten.

Um IntelliCache zu verwenden, müssen Sie es in diesem Produkt und XenServer aktivieren.

- Bei der Installation von XenServer wählen Sie **Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix bietet keine Unterstützung für gemischte Serverpools, auf denen IntelliCache auf manchen Servern aktiviert ist und auf anderen nicht. Weitere Informationen finden Sie in der Dokumentation für XenServer.
- In XenApp und XenDesktop ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur beim Erstellen einer XenServer-Verbindung ändern, IntelliCache kann später nicht deaktiviert werden. Gehen Sie folgendermaßen vor, wenn Sie eine XenServer-Verbindung von Studio aus hinzufügen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

# Verbindungstimer

Sie können mit Richtlinieneinstellungen drei Verbindungstimer konfigurieren:

- **Timer für längste Verbindung:** Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop fest. Verwenden Sie die Richtlinieneinstellungen **Sitzungsverbindungstimer** und **Sitzungsverbindung - Timerintervall**.
- **Timer für inaktive Verbindungen:** Diese Einstellung legt fest, wie lange eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem virtuellen Desktop erhalten wird, wenn keine Eingabe vom Benutzer erfolgt. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- **Timer für getrennte Verbindungen:** Diese Einstellung legt fest, wie lange ein getrennter, gesperrter virtueller Desktop gesperrt bleibt, bis die Sitzung abgemeldet wird. Verwenden Sie die Richtlinieneinstellungen **Timer für getrennte Sitzung** und **Getrennte Sitzungen - Timerintervall**.

Wenn Sie eine dieser Einstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

Weitere Informationen finden Sie in der Dokumentation für die Richtlinieneinstellungen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verbindungsleasing

Jul 08, 2016

Um sicherzustellen, dass die Sitedatenbank immer verfügbar ist, empfiehlt Citrix, unter Befolgung der bewährten Methoden zur hohen Verfügbarkeit von Microsoft mit einer fehlertoleranten SQL Server-Bereitstellung zu beginnen. Delivery Controller können jedoch aufgrund von Netzwerkproblemen und Unterbrechungen möglicherweise nicht auf die Datenbank zugreifen, was dazu führt, dass Benutzer keine Verbindung mit ihren Anwendungen oder Desktops herstellen können.

Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist.

Benutzer verfügen zwar über eine große Anzahl veröffentlichter Ressourcen, verwenden jedoch oft nur wenige davon regelmäßig. Wenn Sie das Verbindungsleasing aktivieren, werden die Benutzerverbindungen mit den zuletzt verwendeten Anwendungen und Desktops im Normalbetrieb (wenn die Datenbank verfügbar ist) von jedem Controller zwischengespeichert.

Die auf jedem Controller generierten Leases werden in die Sitedatenbank für eine regelmäßige Synchronisierung mit den anderen Controllern der Site hochgeladen. Neben den Leases werden in jedem Controllercache Informationen zu Anwendung, Desktop, Symbol und Worker gespeichert. Lease und zugehörige Informationen werden auf dem lokalen Datenträger eines jeden Controllers gespeichert. Wenn die Datenbank nicht mehr verfügbar ist, wechselt der Controller in den Leasingverbindungsmodus und beim Versuch der Herstellung oder des Neuaufbaus einer Verbindung mit einer kürzlich verwendeten Anwendung oder einem kürzlich verwendeten Desktop von StoreFront aus werden die zwischengespeicherten Vorgänge "abgespielt".

Die Verbindungen werden für eine Leasedauer von zwei Wochen zwischengespeichert. Wenn die Datenbank nicht verfügbar ist, besteht daher über StoreFront Zugriff auf die Desktops und Anwendungen, die in den vorherigen zwei Wochen gestartet wurden. Auf Desktops und Anwendungen, die nicht während der zweiwöchigen Leasedauer gestartet wurden, kann jedoch nicht zugegriffen werden, wenn die Datenbank nicht verfügbar ist. Wenn eine Anwendung z. B. vor drei Wochen gestartet wurde, ist ihre Lease abgelaufen und sie kann bei Nichtverfügbarkeit der Datenbank nicht gestartet werden. Leases für langwährende aktive oder getrennte Anwendungen oder Desktopsitzungen werden verlängert und somit nicht als abgelaufen behandelt.

Standardmäßig gilt das Verbindungsleasing für die komplette Site. Sie können jedoch alle Leases für bestimmte Benutzer widerrufen, wodurch verhindert wird, dass diese auf Anwendungen oder Desktops zugreifen können, wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Mehrere weitere Registrierungseinstellungen gelten pro Controller.

## Überlegungen und Einschränkungen

Das Verbindungsleasing kann zwar die Verbindungsresilienz und die Produktivität der Benutzer verbessern, es sind jedoch Überlegungen im Hinblick auf Verfügbarkeit, Betrieb und Leistung anderer Funktionen anzustellen.

Das Verbindungsleasing wird für servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops unterstützt. Es wird nicht unterstützt für gepoolte VDI-Desktops oder Benutzer, denen kein Desktop zugewiesen wurde, wenn die Datenbank betriebsunfähig wird.

Wenn der Controller im Leasingverbindungsmodus ist, gilt Folgendes:

- Administratoren können Studio, Director und die PowerShell-Konsole nicht verwenden.
- Workspace Control ist nicht verfügbar. Wenn sich ein Benutzer bei Citrix Receiver anmeldet, werden Sitzungen nicht


© 1999-2017 Citrix Systems, Inc. All rights reserved.

automatisch wieder verbunden. Der Benutzer muss die Anwendung neu starten.

- Wenn eine neue Lease unmittelbar vor dem Nichtverfügbarwerden der Datenbank erstellt wurde, die Leaseinformationen jedoch noch nicht auf allen Controllern synchronisiert wurden, können Benutzer möglicherweise eine betroffene Ressource nicht starten.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt. Beispiel:
  - Ein Benutzer stellt eine Verbindung von einem Gerät (extern über NetScaler Gateway) her, während der Controller im normalen Verbindungsmodus ist. Später stellt der Benutzer von einem anderen Gerät im LAN eine Verbindung her, während Controller im Leasingverbindungsmodus ist. In diesem Fall findet möglicherweise kein Roaming der Sitzung statt.
  - Die Wiederverbindung einer Sitzung kann fehlschlagen, wenn eine Anwendung startet, kurz bevor die Datenbank betriebsunfähig wird. In diesem Fall werden eine neue Sitzung und Anwendungsinstanz gestartet.
- Bei statischen (zugewiesenen) Desktops findet keine Energieverwaltung statt. VDAs, die beim Umschalten des Controllers in den Leasingverbindungsmodus ausgeschaltet werden, stehen erst wieder zur Verfügung, wenn die Datenbankverbindung wiederhergestellt ist, es sei denn, der Administrator schaltet sie manuell ein.
- Sind Sitzungsvorabstart und Sitzungsfortbestehen aktiviert, werden neue Vorabstartsitzungen nicht gestartet. Vorab gestartete und fortbestehende Sitzungen werden während der Nichtverfügbarkeit der Datenbank nicht entsprechend den konfigurierten Schwellenwerten beendet.
- Die Lastverwaltung der Site kann beeinträchtigt werden. Serverbasierte Verbindungen werden an den zuletzt verwendeten VDA geleitet. Lastauswertungsprogramme (und insbesondere Sitzungszahlregeln) werden möglicherweise überschritten.
- Der Controller wechselt nicht in den Leasingverbindungsmodus, wenn Sie die Datenbank mit SQL Server Management Studio offline nehmen. Verwenden Sie stattdessen eine der folgenden Transact-SQL-Anweisungen:
  - ALTER DATABASE <Datenbankname> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <Datenbankname> SET OFFLINE WITH ROLLBACK AFTER <Sekunden>

  Beide Anweisungen beenden ausstehende Transaktionen und trennen die Verbindung des Controllers mit der Datenbank. Der Controller wechselt dann in den Leasingverbindungsmodus.

Beim Verbindungsleasing gibt es zwei kurze Intervalle, während derer Benutzer keine Verbindung (wieder)herstellen können: (1) zwischen dem Zeitpunkt, zu dem die Datenbank betriebsunfähig wird bis zum Umschalten des Controllers in den Leasingverbindungsmodus und (2) vom Zeitpunkt des Umschaltens des Controllers vom Leasingverbindungsmodus bis der Datenbankzugriff vollständig wiederhergestellt ist und die VDAs erneut registriert sind.

Wenn Sie einen nicht standardmäßigen Wert für das Sitzungsroaming festlegen und ein Controller auf eine geleaste Verbindung schaltet, tritt bei Sitzungswiederverbindung wieder der Standardwert in Kraft. Weitere Informationen finden Sie unter Verbindungsleasing und Sitzungsroaming.

Informationen zum Speicherort der Verbindungsleasingdaten finden Sie in dem Artikel Zonen.

Weitere Überlegungen finden Sie unter XenDesktop 7.6 Connection Leasing Design Considerations.

### Konfigurieren und Bereitstellen

Beim Konfigurieren der Bereitstellung zum Ermöglichen des Verbindungsleasings ist Folgendes zu beachten:

- VDAs müssen mindestens in Version 7.6 und die Maschinenkataloge und Bereitstellungsgruppen, die diese Maschinen verwenden, müssen in der entsprechenden Mindestversion vorliegen.
- Die Speicherplatzanforderungen der Sitedatenbank sind größer.
- Jeder Controller erfordert zusätzlichen Speicherplatz für die zwischengespeicherten Leasedateien.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Das Verbindungsleasing ist standardmäßig aktiviert.

Sie können das Verbindungsleasing im PowerShell-SDK oder in der Windows-Registrierung deaktivieren und aktivieren. Im PowerShell-SDK können Sie auch aktuelle Leases entfernen. Die folgenden PowerShell-Cmdlets wirken sich auf das Verbindungsleasing aus. Informationen hierzu finden Sie in der Cmdlet-Hilfe.

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false: Aktiviert bzw. deaktiviert das Verbindungsleasing. Standard = $true
- Get-BrokerServiceAddedCapability: Gibt "ConnectionLeasing" für den lokalen Controller aus.
- Get-BrokerLease: Ruft alle Leases oder einen gefilterten Satz aktueller Leases auf.
- Remove-BrokerLease: Markiert alle Leases oder einen gefilterten Satz Leases zum Löschen.
- Update-BrokerLocalLeaseCache: aktualisiert den Cache für das Verbindungsleasing auf dem lokalen Controller. Bei der nächsten Synchronisierung werden die Daten neu synchronisiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Virtuelle IP-Adressen und virtuelles Loopback

Jul 08, 2016

Hinweis: Diese Features gelten nur für Maschinen unter Windows Server 2008 R2 und Windows Server 2012 R2. Sie gelten nicht für Windows-Desktopbetriebssystemmaschinen.

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Einige Anwendungen, z. B. CRM oder CTI, verwenden eine IP-Adresse für die Adressierung, Lizenzierung, Identifizierung und andere Zwecke und erfordern daher eine eindeutige IP-Adresse oder eine Loopbackadresse in Sitzungen. Andere Anwendungen binden sich möglicherweise an einen statischen Port an, sodass das Starten weitere Instanzen einer Anwendung in Mehrbenutzerumgebungen fehlschlägt, da der Port bereits verwendet wird. Damit solche Anwendungen in einer XenApp-Umgebung richtig ausgeführt werden können, benötigen Sie für jedes Gerät eine eindeutige IP-Adresse.

Virtuelle IP-Adressen und virtuelles Loopback sind unabhängige Features. Sie können ein Feature oder beide wählen.

Zusammenfassung der Administratoraktion:

- Zur Verwendung von Microsoft virtuellen IPs aktivieren und konfigurieren Sie die Funktion auf dem Windows-Server.
- Für die Verwendung von virtuellem Loopback von Citrix konfigurieren Sie zwei Einstellungen in einer Citrix Richtlinie.

## Virtuelle IP

Wenn die virtuelle IP aktiviert und auf dem Windows-Server konfiguriert ist, scheint jede konfigurierte Anwendung, die in einer Sitzung ausgeführt wird, eine eindeutige Adresse zu haben. Benutzer greifen auf diese Anwendungen auf einem XenApp-Server genauso wie auf andere veröffentlichte Anwendungen zu. Ein Prozess erfordert die virtuelle IP in den folgenden Fällen:

- Der Prozess verwendet eine hartcodierte TCP-Portnummer
- Der Prozess verwendet Windows Sockets und benötigt eine eindeutige IP-Adresse oder eine angegebene TCP-Portnummer

Ermitteln, ob eine Anwendung virtuelle IP-Adressen verwenden muss

1. Beziehen Sie das TCPView-Tool von Microsoft. Das Programm zeigt alle Anwendungen an, die an spezifische IP-Adressen und Ports binden.
2. Deaktivieren Sie das Auflösen von IP-Adressen, sodass statt der Adressen die Hostnamen angezeigt werden.
3. Starten Sie die Anwendung und ermitteln Sie mit TCPView, welche IP-Adressen und Ports von der Anwendung geöffnet werden und welche Prozesse diese Ports öffnen.
4. Konfigurieren Sie alle Prozesse, die die IP-Adresse des Servers, 0.0.0.0 oder 127.0.0.1, öffnen.
5. Starten Sie eine zusätzliche Instanz der Anwendung, um sicherzustellen, dass sie nicht dieselbe IP-Adresse auf einem anderen Port öffnet.

**Funktionsweise von Microsoft Remote Desktop-Virtualisierung**

- Die virtuelle IP-Adressierung muss auf dem Microsoft Server aktiviert sein.
  Beispiel: In einer Umgebung mit Windows Server 2008 R2 erweitern Sie im Server-Manager "Remotedesktopdienste > Remotedesktop-Sitzungshostverbindungen", um das Remotedesktop-IP-Virtualisierungsfeature zu aktivieren, und konfigurieren Sie die Einstellungen so, dass IP-Adressen dynamisch mit dem DHCP-Server pro Sitzung oder pro Programm zugewiesen werden. Weitere Informationen finden Sie in der Microsoft Dokumentation.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Nach der Aktivierung des Features fordert der Server beim Sitzungsstart dynamisch zugewiesene IP-Adressen vom DHCP-Server an.
- Das Remotedesktop-IP-Virtualisierungsfeature weist den Remotedesktopverbindungen die IP-Adressen pro Sitzung oder pro Programm zu. Wenn Sie IP-Adressen für mehrere Programme zuweisen, verwenden sie eine gemeine IP-Adresse pro Sitzung.
- Wenn einer Sitzung eine Adresse zugewiesen wurde, verwendet die Sitzung die virtuelle Adresse statt der primären IP-Adresse des Systems bei den folgenden Aufrufen: Bind, Closesocket, Connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Wenn das IP-Virtualisierungsfeature von Microsoft in der Hostingkonfiguration der Remotedesktopsitzung verwendet wird, sind Anwendungen an bestimmte IP-Adressen gebunden, indem eine Filterkomponente zwischen die Anwendung und den Winsock-Funktionsaufrufen eingefügt wird. Die Anwendung erkennt dann nur die IP-Adresse, die sie verwenden soll. Sollte die Anwendung versuchen, TCP- oder UDP-Kommunikation abzuhören, wird sie automatisch an die zugewiesene virtuelle IP-Adresse (oder Loopbackadresse) gebunden und alle von der Anwendung geöffneten Ausgangsverbindungen gehen von der an die Anwendung gebundene IP-Adresse aus.

In Funktionen, die eine Adresse ausgeben, wie z. B. GetAddrInfo() (über eine Windows--Richtlinie gesteuert), untersucht die virtuelle IP beim Abrufen der IP-Adresse des lokalen Hosts die zurückgegebene IP-Adresse und ändert sie in die virtuelle IP-Adresse der Sitzung. Anwendungen, die mit solchen Namensfunktionen versuchen, die IP-Adresse des lokalen Servers zu ermitteln, erhalten nur die eindeutige virtuelle IP-Adresse, die der Sitzung zugeordnet wurde. Diese IP-Adresse wird oft in späteren Socket-Aufrufen, wie "Bind" oder "Connect", verwendet.

Oft fordern Anwendungen eine Bindung an einen Port zum Abhören der Adresse 0.0.0.0. Wenn eine Anwendung dies versucht und einen statischen Port verwendet, können Sie höchstens eine Instanz der Anwendung starten. Das virtuelle IP-Adressfeature sucht in diesen Aufrufen nach 0.0.0.0 und ändert den Abruf so, dass die angegebene virtuelle IP-Adresse abgehört wird. Dies ermöglicht, dass mehrere Anwendungen denselben Port auf demselben Computer abhören, da sie auf verschiedenen Adressen abhören. Der Aufruf wird nur geändert, wenn er in einer ICA-Sitzungen erfolgt und virtuelle IP-Adressen aktiviert sind. Beispiel: Wenn zwei Instanzen einer Anwendung, die in unterschiedlichen Sitzungen ausgeführt werden, eine Bindung mit allen Schnittstellen (0.0.0.0) und einen bestimmten Port (z. B. 9000) versuchen, werden sie an VIPAddress1:9000 und VIPAddress2:9000 gebunden und es gibt keinen Konflikt.

### Virtuelles Loopback

Bei Aktivierung der Citrix Richtlinieneinstellungen für virtuelles Loopback kann jede Sitzung eine eigene Loopbackadresse für die Kommunikation haben. Verwendet eine Anwendung in einem Winsock-Aufruf die Adresse des lokalen Hosts (Standard ist 127.0.0.1), ersetzt das virtuelle Loopback die Adresse 127.0.0.1 einfach durch 127.X.X.X ersetzt, wobei X.X.X die Sitzungs-ID + 1 ist. Wenn die Sitzungs-ID zum Beispiel 7 ist, ist die Adresse 127.0.0.8. Im unwahrscheinlichen Fall, dass die Sitzungs-ID größer ist, als im vierten Oktett zulässig (mehr als 255), wird beim nächsten Oktett weitergemacht (127.0.1.0) bis zum Maximum von 127.255.255.255.

Ein Prozess erfordert das virtuelle Loopback in den folgenden Fällen:
- Der Prozess verwendet die Windows- Sockets-Loopbackadresse (localhost) (127.0.0.1)
- Der Prozess verwendet eine hartcodierte TCP-Portnummer

Verwenden Sie die Richtlinieneinstellungen für virtuelles Loopback für Anwendungen, die eine Loopbackadresse für prozessübergreifende Kommunikation verwenden. Eine zusätzliche Konfiguration ist nicht erforderlich. Virtuelles Loopback ist nicht von virtueller IP abhängig, sodass der Microsoft-Server nicht konfiguriert werden muss.
- Virtuelle IP - Loopbackunterstützung: Wenn diese Richtlinieneinstellung aktiviert ist, kann jede Sitzung eine eigene virtuelle Loopbackadresse haben. Diese Einstellung ist standardmäßig aktiviert. Das Feature gilt nur für Anwendungen, die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

mit der Richtlinieneinstellung Virtuelle IP - Programme für virtuelles Loopback angegeben wurden.
- Virtuelle IP - Programme für virtuelles Loopback: Mit dieser Richtlinieneinstellung geben Sie die Anwendung an, die das Feature "Virtuelles IP-Loopback" verwenden. Diese Einstellung gilt nur, wenn die Richtlinieneinstellung Virtuelle IP - Loopbackunterstützung aktiviert ist.

**Verwandtes Feature**

Mit den folgenden Registrierungseinstellungen stellen Sie sicher, dass virtuelles Loopback den Vorrang vor virtuelle IP erhält; dies wird als bevorzugtes Loopback bezeichnet. Achten Sie jedoch auf Folgendes:
- Bevorzugtes Loopback wird nur unter Windows 2008 R2 unterstützt.
- Verwenden Sie bevorzugtes Loopback nur, wenn virtuellen IP-Adressen und das virtuelle Loopback aktiviert sind, sonst erhalten Sie u. U. unerwartete Ergebnisse.
- Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Führen Sie regedit auf den Servern aus, auf dem die Anwendungen installiert sind.
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP für 32-Bit-Maschinen)
- Name: PreferLoopback, Typ: REG_DWORD, Wert: 1
- Name: PreferLoopbackProcesses, Typ: REG_MULTI_SZ Wert:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Delivery Controller

Aug 17, 2016

Der Delivery Controller ist die serverseitige Komponente, die für die Verwaltung des Benutzerzugriffs sowie das Brokering und Optimieren von Verbindungen zuständig ist. Controller stellen auch die Maschinenerstellungsdienste zur Erstellung von Desktop- und Serverimages bereit.

Eine Site muss mindestens über einen Controller verfügen. Nach der Installation des ersten Controllers können Sie im Rahmen der Siteerstellung oder auch später weitere Controller hinzufügen. Es gibt zwei Hauptvorteile, mehr als einen Controller in einer Site zu haben.

- Redundanz: Als bewährte Methode sollte eine Produktionssite immer mindestens zwei Controller auf unterschiedlichen physischen Servern haben. Wenn ein Controller ausfällt, können die anderen die Verwaltung der Verbindungen und der Site übernehmen.
- Skalierbarkeit: Je intensiver die Aktivität einer Site, umso mehr nehmen CPU-Auslastung auf dem Controller und die Datenbankaktivität zu. Zusätzliche Controller bieten die Möglichkeit, mehr Benutzer, Anwendungen und Desktopanforderungen zu verarbeiten und die Reaktionszeit insgesamt zu verbessern.

Jeder Controller kommuniziert direkt mit der Sitedatenbank. In einer Site mit mehreren Zonen kommunizieren die Controller in jeder Zone mit der Datenbank in der primären Zone.

**Tipp:** Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers, nachdem Sie die Site konfiguriert haben.

# Erkennen von Controllern durch VDAs

VDAs können erst verwendet werden, wenn sie bei einem Controller der Site registriert wurden (Herstellen der Kommunikation). Zur Suche eines Controllers überprüft der VDA die Controllerliste "ListofDDCs". Die Liste "ListOfDDCs" enthält einen oder mehrere DNS-Einträge oder IP-Adressen, die den VDA an die Controller der Site verweisen. Um einen Lastausgleich zu erzielen, verteilt der VDA die Verbindungen automatisch über alle Controller in der Liste.

Neben der Liste "ListOfDDCs" gibt es die Liste "ListOfSIDs", in der festgelegt ist, über welche Sicherheits-IDs (SIDs) der VDA als Controller angesprochen werden kann. Die Liste "ListOfSIDs" kann verwendet werden, um die Last auf Active Directory zu verringern oder um Sicherheitsbedrohungen durch einen nicht sicheren DNS-Server zu vermeiden.

Die Listen "ListOfDDCs" und "ListOfSIDs" müssen auf allen VDAs auf dem neuesten Stand sein, wenn Controller in der Site hinzugefügt und entfernt werden. Sind die Listen nicht aktuell, werden Sitzungsstarts, die durch einen nicht aufgeführten Controller vermittelt werden, vom VDA möglicherweise abgelehnt. Ungültige Einträge in der Liste können den Start der Systemsoftware des virtuellen Desktops verzögern. Halten Sie die Listen wie folgt auf dem neuesten Stand:

- Verwenden Sie automatische Updates zur automatischen Aktualisierung der Listen "ListOfDDCs" und "ListOfSIDs", wenn Controller hinzugefügt oder entfernt werden. Standardmäßig sind automatische Updates aktiviert.
- Eigenverwaltung: Aktualisieren Sie die Richtlinien- oder Registrierungseinstellungen für die Controller manuell.

Die Informationen in den Listen "ListOfDDCs" und "ListOfSIDs" können aus verschiedenen Orten der Bereitstellung stammen. Folgende Speicherorte werden vom VDA nacheinander überprüft, bis die Listen gefunden werden:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Ein Speicherort für den persistenten Speicher für automatische Updates. Dieser Speicherort enthält die Controllerinformationen, wenn automatische Updates aktiviert sind und nachdem der VDA erfolgreich zum ersten Mal nach der Installation registriert wurde. (Der Speicher enthält zudem Maschinenrichtlinieninformationen, damit Richtlinieneinstellungen bei Neustarts beibehalten werden.) Bei der ersten Registrierung nach der Installation, oder wenn automatische Updates deaktiviert sind, prüft der VDA die nachfolgend aufgeführten Stellen.
2. Richtlinieneinstellungen (Controller, Controller-SIDs).
3. Controllerinformationen des Virtual Desktop Agent-Schlüssels in der Registrierung. Diese Werte stammen ursprünglich vom VDA-Installationsprogramm, basierend auf den Controllerinformationen, die Sie bei der Installation des VDAs eingeben.
4. Auf Organisationseinheiten basierende Controller-Discovery. Dies ist eine ältere Methode die zugunsten der Abwärtskompatibilität beibehalten wird.
5. Die durch die Maschinenerstellungsdienste erstellte Datei Personality.ini.

Wenn in ListOfDDCs mehrere Controller angegeben sind, erfolgt die Verbindung mit ihnen durch den VDA in einer zufälligen Reihenfolge. Die Liste "ListOfDDCs" kann auch Controllergruppen enthalten, die an den Klammern um zwei oder mehr Controllereinträge zu erkennen sind. Der VDA versucht, eine Verbindung mit jedem Controller in einer Gruppe herzustellen, bevor er weitere Einträge in der Liste "ListOfDDCs" versucht.

Für XenDesktop-Benutzer, die ein Upgrade einer Version vor 7.0 durchgeführt haben, ersetzt das Feature für automatische Updates die CNAME-Funktion der Vorversion. Sie können die CNAME-Funktion ggf. wieder aktivieren, jedoch funktioniert das DNS-Aliasing nur konsistent, wenn Sie das AutoUpdate-Feature und die CNAME-Funktion nicht zusammen verwenden. Weitere Informationen zum erneuten Aktivieren der CNAME-Funktion finden Sie unter CTX137960.

Informationen zu den Zielorten der VDA-Registrierung in Sites mit mehreren Zonen finden Sie im Artikel "Zonen".

# Überlegungen zur Verwendung automatischer Updates oder der Eigenverwaltung

Die Richtlinieneinstellung zur Aktivierung/Deaktivierung der automatischen Updates ist standardmäßig aktiviert.

Bei folgenden Bereitstellungstypen sind keine automatischen Updates möglich, stattdessen muss die Eigenverwaltung verwendet werden:

- Bereitstellungen mit Controllergruppen
- Bereitstellungen, die aus Sicherheitsgründen ListOfSIDs verwenden (Bei Bereitstellungen mit ListOfSIDs zur Verringerung der Active Directory-Last können automatische Updates verwendet werden)
- Bereitstellungen, die Provisioning Services ohne Datenträger für Zurückschreiben verwenden
- Bereitstellungen, die die Controller- oder Controller-SIDs-Richtlinieneinstellung verwenden

# Automatische Updates

Die Richtlinieneinstellung *Automatische Controllerupdates aktivieren* ist Teil der Kategorie "Virtual Delivery Agent". Zum Aktivieren automatischer Updates aktivieren Sie die Richtlinieneinstellung (standardmäßig aktiviert). Zum Deaktivieren automatischer Updates deaktivieren Sie die Richtlinieneinstellung

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Wird bei aktivierten automatischen Updates ein VDA installiert, versucht der VDA, sich mit einem der Controller-Werte zu registrieren, die bei der Installation des VDAs von Ihnen eingegeben wurden. Das Installationsprogramm schreibt die Controllerinformationen, die Sie bei der Installation des VDAs angegeben haben, in den Registrierungswert "ListOfDDCs".

Nach der VDA-Registrierung sendet der Controller, bei dem die Registrierung erfolgte, eine Liste der vollständig qualifizierten Domänennamen (FQDNs) und Sicherheits-IDs (SIDs) an den VDA. Der VDA schreibt diese Liste in den persistenten Speicher für automatische Updates. Die Sitekonfigurationsdatenbank wird alle 90 Minuten von jedem Controller auf Controllerinformationen überprüft: Wenn seit der letzten Überprüfung ein Controller hinzugefügt oder entfernt wurde oder wenn eine Richtlinie geändert wurde, wird die aktualisierte Liste vom Controller an die registrierten VDAs gesendet. Der VDA nimmt alle Verbindungen von allen Controllern in der aktuellen Liste an.

Geht eine Liste ein, die den Controller, bei dem der VDA registriert ist, nicht enthält (d. h. der Controller wurde aus der Site entfernt), nimmt der VDA eine neue Registrierung bei einem der Controller aus der Liste vor. Nach der Registrierung bzw. Neuregistrierung erhält der VDA eine aktualisierte Liste.

Beispiel:

1. Eine Bereitstellung hat drei Controller: A, B und C. Ein VDA ist installiert und wird bei Controller B registriert (dies wurde bei der Installation des VDAs festgelegt).
2. Zwei Controller (D und E) werden der Site hinzugefügt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen und können Verbindungen von Controllern A, B, C, D und E annehmen. (Die Last wird erst nach Neustart der VDAs gleichmäßig auf alle Controller verteilt.)
3. Controller B wird aus der Site entfernt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen, da seit der letzten Überprüfung eine Controlleränderung stattfand. Der in Schritt 1 installierte VDA ist bei Controller B registriert, der jedoch in der Liste nicht mehr enthalten ist. Somit wird der VDA bei einem der anderen Controller der Liste (A, C, D und E) neu registriert.

# Eigenverwaltung

Wenn Sie keine automatischen Updates verwenden, müssen Sie die Citrix Richtlinieneinstellung oder die Registrierungswerte für jeden VDA der Site aktualisieren, wenn Delivery Controller in der Site hinzugefügt, verschoben oder entfernt wurden. Registrierungsänderungen können auch mit dem Gruppenrichtlinienobjekt aktualisiert werden.

Verwenden der Eigenverwaltung mit Citrix Richtlinieneinstellungen

1. Aktualisieren Sie die vollqualifizierten Domänennamen in der Richtlinieneinstellung "Controller". Diese Richtlinieneinstellung ist in der Kategorie "Virtual Delivery Agent".
2. Wenn Sie in Ihrer Bereitstellung auch ListOfSIDs-Listen verwenden, aktualisieren Sie die SID-Werte der Einstellung "Controller SIDspolicy".

Verwenden der Eigenverwaltung mit der Registrierung

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Aktualisieren Sie den Registrierungsschlüssel "ListOfDDCs", der die vollqualifizierten Domänennamen aller Controller in der Site enthält. (Dieser Schlüssel entspricht der Active Directory-Site-Organisationseinheit.) Trennen Sie mehrere Werte mit

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Leerzeichen. Umschließen Sie Controllergruppen mit Klammern.
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

Wenn die Registrierungsstruktur HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent sowohl die Registrierungsschlüssel "ListOfDDCs" und "FarmGUID" enthält, wird ListOfDDCs für Controller-Discovery verwendet; FarmGUID ist vorhanden, wenn die Organisationseinheit der Site bei der Installation des VDAs angegeben wurde.

2. Aktualisieren Sie wahlweise den Registrierungsschlüssel "ListOfSIDs":
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

# Hinzufügen, Entfernen oder Verschieben von Controllern

Zum Hinzufügen, Entfernen oder Verschieben eines Controllers benötigen Sie die im Artikel "Datenbanken" aufgeführten Serverrollen- und Datenbankrollenberechtigungen.

**Hinweis:** Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Wenn in der Bereitstellung Datenbankspiegelung verwendet wird, gilt Folgendes:

- Vor dem Hinzufügen, Entfernen oder Verschieben von Controllern müssen Sie sicherstellen, dass sowohl die gespiegelte als auch die Hauptdatenbank ausgeführt werden. Wenn Sie mit Skripts für SQL Server Management Studio arbeiten, müssen Sie den SQLCMD-Modus vor dem Ausführen des Skripts aktivieren.
- Zum Prüfen der Spiegelung nach dem Hinzufügen, Entfernen oder Verschieben des Controllers führen Sie das PowerShell-Cmdlet **get-configdbconnection** aus, um sicherzustellen, dass der Failoverpartner in der Verbindungszeichenfolge für die Spiegelung eingerichtet wurde.

Gehen Sie nach dem Hinzufügen, Entfernen oder Verschieben eines Controllers wie folgt vor:

- Wenn das automatische Update aktiviert ist, erhalten die VDAs eine aktualisierte Liste der Controller innerhalb von 90 Minuten.
- Ist das automatische Update nicht aktiviert, müssen Sie sicherstellen, dass die Controllerrichtlinieneinstellung oder der Registrierungsschlüssel "ListOfDDCs" für alle VDAs aktualisiert wird. Nachdem Sie einen Controller in eine andere Site verschoben haben, müssen Sie die Richtlinieneinstellung oder den Registrierungsschlüssel in beiden Sites aktualisieren.

## Hinzufügen eines Controllers

Sie können Controller bei der Siteerstellung oder zu einem späteren Zeitpunkt hinzufügen. Sie können einer Site, die mit dieser Softwareversion erstellt wurde, keine Controller hinzufügen, die mit einer früheren Version installiert wurden.

1. Führen Sie das Installationsprogramm auf einem Server mit einem unterstützten Betriebssystem aus. Installieren Sie den Delivery Controller und alle anderen gewünschten Kernkomponenten. Führen Sie die Schritte des Installationsassistenten durch.
2. Wenn Sie noch keine Site erstellt haben, starten Sie Studio; Sie werden aufgefordert, eine Site zu erstellen. Klicken Sie auf der Seite "Datenbanken" im Assistenten für die Siteerstellung auf die Schaltfläche "Auswählen" und fügen Sie die Adresse des Servers hinzu, auf dem Sie den zusätzlichen Controller installiert haben. **Wichtig**: Wenn Sie Skripts zur Initialisierung der Datenbanken generieren möchten, fügen Sie die Controller vor Generieren der Skripts hinzu.
3. Wenn Sie bereits eine Site erstellt haben, verweisen Sie Studio auf den Server, auf dem Sie den zusätzlichen Controller installiert haben. Klicken Sie auf **Bereitstellung erweitern** und geben Sie die Siteadresse ein.

## Entfernen eines Controllers

Beim Entfernen eines Controllers aus einer Site werden die Citrix Software und andere Komponenten nicht deinstalliert. Es wird lediglich der Controller aus der Datenbank entfernt, der damit für das Brokering von Verbindungen oder sonstige


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aufgaben nicht mehr verfügbar ist. Wenn Sie einen Controller entfernen, können Sie diesen zu einem späteren Zeitpunkt der gleichen oder einer anderen Site wieder hinzufügen. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.

Wenn Sie einen Controller von einer Site entfernen, wird die Controller-Anmeldung für den Datenbankserver nicht entfernt. Auf diese Weise wird vermieden, dass eine Anmeldung entfernt wird, die von den Diensten anderer Produkte auf demselben Computer verwendet wird. Die Anmeldung muss manuell entfernt werden, wenn sie nicht mehr erforderlich ist. Dazu benötigen Sie die Berechtigungen der securityadmin-Serverrolle.

**Wichtig:** Entfernen Sie den Controller erst dann aus Active Directory, wenn Sie ihn aus der Site entfernt haben.

1. Stellen Sie sicher, dass der Controller eingeschaltet ist, sodass Studio in weniger als einer Stunde geladen wird. Wenn Studio den Controller lädt, den Sie entfernen möchten, schalten Sie den Controller aus, wenn Sie dazu aufgefordert werden.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller, den Sie entfernen möchten.
3. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem der Datenbankadministrator den Controller für Sie entfernen kann.
4. Möglicherweise müssen Sie das Maschinenkonto des Controllers auf dem Datenbankserver entfernen. Bevor Sie dies durchführen, überprüfen Sie, ob das Konto von einem anderen Dienst verwendet wird.

Nachdem Sie mit Studio einen Controller entfernt haben, besteht ggf. kurze Zeit weiter Datenverkehr zu diesem Controller, um sicherzustellen, dass die aktuellen Tasks einwandfrei abgeschlossen werden. Wenn Sie das Entfernen eines Controllers in sehr kurzer Zeit erzwingen möchten, empfiehlt Citrix, den Server, auf dem er installiert war, herunterzufahren oder aus Active Directory zu entfernen. Starten Sie dann die anderen Controller in der Site neu, um sicherzustellen, dass keine weitere Kommunikation mit dem entfernten Controller stattfindet.

### Verschieben eines Controllers in eine andere Zone

Wenn die Site mehrere Zonen enthält, können Sie Controller in eine andere Zone verschieben. Informationen zu den Auswirkungen des Verschiebens auf die VDA-Registrierung und andere Vorgänge finden Sie im Artikel "Zonen".

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller aus, den Sie verschieben möchten.
2. Wählen Sie im Aktionsbereich **Verschieben**.
3. Geben Sie die Zone an, in die Sie den Controller verschieben möchten.

### Verschieben eines Controllers in eine andere Site

Controller können nicht in eine Site verschoben werden, die mit einer früheren Version dieser Software erstellt wurde.

1. Wählen Sie in der derzeitigen Site des Controllers (der alten Site) im Studio-Navigationsbereich **Konfiguration > Controller** und wählen Sie anschließend den Controller aus, den Sie verschieben möchten.
2. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem eine Person mit den entsprechenden Berechtigungen, (z. B. der Datenbankadministrator) den Controller für Sie entfernen kann. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.
3. Öffnen Sie Studio auf dem zu verschiebenden Controller, setzen Sie bei entsprechender Aufforderung die Dienste zurück, wählen Sie **Vorhandener Site beitreten** und geben Sie die Adresse der neuen Site ein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

### Verschieben eines VDA in eine andere Site

Wenn ein VDA mit Provisioning Services bereitgestellt wurde oder wenn er ein vorhandenes Image ist, können Sie einen VDA in eine andere Site (von Site 1 nach Site 2) verschieben, wenn Sie ein Upgrade vornehmen oder wenn Sie ein in einer Testsite erstelltes VDA-Image in eine Produktionssite verschieben. Mit Maschinenerstellungsdienste (MCS) bereitgestellte VDAs können nicht zwischen Sites verschoben werden, da MCS das Ändern der ListOfDDCs nicht unterstützt, die ein VDA zum Registrieren mit einem Controller prüft. Mit Maschinenerstellungsdienste bereitgestellte VDAs prüfen immer die ListOfDDCs, die der Site zugeordnet ist, in der sie erstellt wurden.

Es gibt zwei Möglichkeiten, einen VDA in eine andere Site zu verschieben: mit dem Installationsprogramm oder mit Citrix Richtlinien.

Installationsprogramm: Führen Sie das Installationsprogramm aus und fügen Sie einen Controller hinzu, wobei Sie in Site 2 einen vollqualifizierten Domänennamen (DNS-Eintrag) eines Controllers angeben. **Wichtig:** Geben Sie Controller im Installationsprogramm nur dann an, wenn die Richtlinieneinstellung "Controller" nicht verwendet wird.

Gruppenrichtlinienobjekt-Editor: Im folgenden Beispiel werden mehrere VDAs verschoben.

1. Erstellen Sie eine Richtlinie in Site 1 mit den nachfolgenden Einstellungen und filtern Sie die Richtlinie auf Bereitstellungsgruppenebene, um eine mehrstufige VDA-Migration zwischen den Sites zu erzielen.
   Controller: mit vollqualifizierten Domänennamen (DNS-Einträgen) von einem oder mehreren Controllern der Site 2.
   Automatische Controllerupdates aktivieren: auf "Deaktiviert" gesetzt.
2. Jeder VDA in der Bereitstellungsgruppe wird innerhalb von 90 Minuten auf die neue Richtlinie hingewiesen. Der VDA ignoriert die eingegangene Liste der Controller (da automatische Updates deaktiviert sind) und wählt einen der in der Richtlinie angegebenen Controller, d. h. einen der Controller in Site 2.
3. Wenn der VDA erfolgreich bei einem Controller der Site 2 registriert wurde, empfängt er die Liste "ListOfDDCs" und die Richtlinieninformationen von Site 2, für die automatische Updates standardmäßig aktiviert sind. Da der Controller, bei dem der VDA in Site 1 registriert war, nicht in der vom Controller in Site 2 gesendeten Liste ist, erfolgt eine erneute Registrierung des VDAs unter Auswahl eines Controllers der Liste von Site 2. Ab sofort wird der VDA automatisch mit Informationen von Site 2 aktualisiert.

# Auf Organisationseinheiten von Active Directory-basierte Controller-Discovery

Diese Delivery Controller-Erkennungsmethode wird vor allem unterstützt, um Abwärtskompatibilität zu gewährleisten. Sie gilt nur für Virtual Delivery Agents (VDAs) für Windows-Desktopbetriebssysteme, aber nicht für VDAs für Windows-Serverbetriebssysteme. Bei der Active Directory-basierten Discovery müssen alle Computer in einer Site Mitglied einer Domäne sein und zwischen der Domäne, die vom Controller verwendet wird, und den von den Desktops verwendeten Domänen muss eine Vertrauensstellung bestehen. Wenn Sie diese Methode verwenden, müssen Sie die GUID der Organisationseinheit in jeder Desktopregistrierung konfigurieren.

Führen Sie für eine auf Organisationseinheiten basierende Controller-Discovery das PowerShell-Skript Set-ADControllerDiscovery.ps1 auf dem Controller aus (das Skript ist auf jedem Controller im Ordner $Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). Um das Skript auszuführen, müssen Sie über CreateChild-Berechtigungen für eine übergeordnete Organisationseinheit verfügen sowie über vollständige Administratorrechte.

Wenn Sie eine Site erstellen, müssen Sie eine entsprechende Organisationseinheit in Active Directory erstellen, wenn


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Desktops die Controller in der Site mit Active Directory ermitteln sollen. Die Organisationseinheit kann in jeder Domäne in der Gesamtstruktur erstellt werden, die Ihre Computer enthält. Optimalerweise sollte die Organisationseinheit auch die Controller der Site enthalten; dies wird jedoch nicht erzwungen bzw. ist nicht erforderlich. Ein Domänenadministrator mit den entsprechenden Privilegien kann die Organisationseinheit als leeren Container erstellen und dann Administrationsrechte an der Organisationseinheit an einen Citrix Administrator delegieren.

Das Skript erstellt einige wichtige Objekte. Nur Active Directory-Standardobjekte werden erstellt und verwendet. Es ist nicht erforderlich, das Schema zu erweitern.

- Eine Controller-Sicherheitsgruppe. Das Computerkonto aller Controller in der Site muss ein Mitglied dieser Sicherheitsgruppe sein. Desktops in einer Site nehmen nur Daten von Controllern an, die Mitglied dieser Sicherheitsgruppe sind.
  Stellen Sie sicher, dass alle Controller auf allen virtuellen Desktops, auf denen der VDA ausgeführt wird, die Berechtigung "Auf diesen Computer vom Netzwerk aus zugreifen" haben. Geben Sie hierfür der Controller-Sicherheitsgruppe dieses Privileg. Wenn Controller nicht über diese Berechtigung verfügen, werden VDAs nicht registriert.

- Ein Dienstverbindungspunkt-Objekt, das Informationen zur Site enthält, wie den Namen der Site. Wenn Sie eine Organisationseinheit der Site mit dem Verwaltungstool "Active Directory-Benutzer und -Computer" prüfen, müssen Sie ggf. "Erweiterte Funktionen" im Menü "Ansicht" aktivieren, um Dienstverbindungspunkt-Objekte anzuzeigen.
- Einen "RegistrationServices" genannten Container, der in der Organisationseinheit der Site erstellt wird. Dieser Container enthält ein Dienstverbindungspunkt-Objekt für jeden Controller in der Site. Bei jedem Start des Controllers wird der Inhalt des Dienstverbindungspunkts geprüft und ggf. aktualisiert.

Wenn nach dem Abschluss der Erstinstallation mehrere Administratoren Controller hinzufügen oder entfernen, benötigen sie Berechtigungen zum Erstellen und Löschen von untergeordneten Objekten für den RegistrationServices-Container und zum Schreiben der Eigenschaften der Controller-Sicherheitsgruppe (diese Berechtigungen werden automatisch dem Administrator gewährt, der das Skript "Set-ADControllerDiscovery.ps1" ausführt). Der Domänenadministrator oder der Administrator der Originalinstallation kann diese Berechtigungen zuweisen; Citrix empfiehlt, dass Sie eine Sicherheitsgruppe für diesen Zweck einrichten.

Wenn Sie eine Organisationseinheit der Site verwenden:

- Informationen werden nur bei der Installation oder Deinstallation dieser Software in Active Directory geschrieben oder wenn beim Start eines Controllers die Informationen im Dienstverbindungspunkt aktualisiert werden müssen (der Controller wurde beispielsweise umbenannt oder der Kommunikationsport wurde geändert). In der Standardeinstellung erstellt das Skript "Set-ADControllerDiscovery.ps1" die richtigen Berechtigungen für die Organisationseinheit der Site und gibt jedem Controller Schreibrechte für den Dienstverbindungspunkt. Mit dem Inhalt der Objekte in der Organisationseinheit der Site wird eine Vertrauensstellung zwischen Desktops und Controllern erstellt. Stellen Sie Folgendes sicher:
  - Nur autorisierte Administratoren können der Controller-Sicherheitsgruppe über die Zugriffssteuerungsliste der Sicherheitsgruppe Computer hinzufügen oder Computer aus der Gruppe entfernen.
  - Nur autorisierte Administratoren und der relevante Controller können Informationen im Dienstverbindungspunkt des Controllers ändern.
- Bei einer Bereitstellung mit Replikation entstehen möglicherweise Verzögerungen; Weiteres hierzu finden Sie in der Microsoft Dokumentation. Dies ist besonders wichtig, wenn Sie die Organisationseinheit der Site in einer Domäne erstellen, die Domänencontroller in mehreren Active Directory-Sites enthält. Abhängig vom Standort der Desktops, der Controller und der Domänencontroller sind Änderungen, die Sie an Active Directory beim erstmaligen Erstellen der Organisationseinheit der Site, beim Installieren oder Deinstallieren von Controllern oder beim Ändern von Controllernamen

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

oder Kommunikationsports vornehmen, erst nach der Replikation auf den entsprechenden Domänencontroller für Desktops erkennbar. Symptome einer solchen Replikationsverzögerung sind u. a. Desktops, die keine Verbindung mit Controllern herstellen können und daher nicht für Benutzerverbindungen verfügbar sind.
- Diese Software verwendet mehrere standardmäßige Computerobjektattribute in Active Directory zum Verwalten von Desktops. Je nach Bereitstellung kann der vollqualifizierte Domänenname des Maschinenobjekts so wie er im Active Directory-Datensatz des Desktops gespeichert ist in den Verbindungseinstellungen eingeschlossen werden, die an den Benutzer zum Herstellen einer Verbindung zurückgegeben werden. Stellen Sie sicher, dass diese Informationen mit den Informationen in der DNS-Umgebung übereinstimmen.

Zum Verschieben eines Controllers in eine andere Site mithilfe der OU-basierten Controller-Discovery befolgen Sie die o. a. Anweisungen für das Verschieben von Controllern. Nach dem Entfernen des Controllers aus der alten Site (Schritt 2) führen Sie das PowerShell-Skript **Set-ADControllerDiscovery –sync** aus. Das Skript synchronisiert die Organisationseinheit mit dem aktuellen Satz an Controllern. Nach dem Beitritt zur vorhandenen Site (Schritt 3), führen Sie das gleiche Skript auf einem Controller in der neuen Site aus.

## Erforderliche Berechtigungen für auf Organisationseinheiten basierende Discovery

Die erforderlichen Berechtigungen hängen von den Aktionen ab und wer oder was Berechtigungen benötigt.

**Während der Siteerstellung**

Der Citrix Siteadministrator, der das Skript "Set-ADControllerDiscovery.ps1" ausführt, benötigt Rechte für die Organisationseinheiten (OU) der Site, um untergeordnete Organisationseinheiten und Objekte zu erstellen. (Wenn keine Organisationseinheit für die Site vorhanden ist, benötigt der Administrator die Rechte, eine zu erstellen. Citrix empfiehlt, dass der AD-Domänenadministrator diese Organisationseinheit vorab erstellt und dann dem Citrix Siteadministrator dafür die Rechte zuweist.) Die erforderlichen Rechte innerhalb der Organisationseinheit sind die Folgenden:

- SCP erstellen
- Container erstellen
- Sicherheitsgruppe erstellen

Das Skript kann auch die Organisationseinheit für die Site erstellen. Dazu benötigt der Administrator das Recht zum Erstellen von Organisationseinheiten für die übergeordnete Organisationseinheit der neuen Organisationseinheit. Wie zuvor erwähnt empfiehlt Citrix dies jedoch nicht.

In diesem Fall ist der Benutzer implizit der Eigentümer der erstellten Elemente, daher benötigen Sie keine zusätzlichen Unterberechtigungen für diese Elemente. Jetzt sollten auch alle zusätzlichen Eigenschaften der neu erstellten Sicherheitsgruppe festgelegt werden.

**Beim Hinzufügen oder Entfernen eines Controllers**

Der Citrix Siteadministrator kann das Skript "ADControllerDiscovery.ps1" ausführen und damit der Site einen Controller hinzufügen oder einen Controller von der Site entfernen. Dies kann ein anderer Administrator sein als der, der den Inhalt der Organisationseinheit ursprünglich erstellt hat. Folgende Rechte sind erforderlich:

- Maschine der Sicherheitsgruppe des Controllers hinzufügen/daraus entfernen
- SCP im Container "RegistrationServices" erstellen/löschen

**Bei normalem Betrieb**

Bei normalem Betrieb benötigen Controller-Maschinen und VDA-Maschinen die folgenden Rechte:

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- Controller benötigen Rechte zum Festlegen von Eigenschaften auf dem eigenen SCP-Objekt (im Container "RegistrationServices")
- Controller und VDAs benötigen Rechte für alle Objekte in der Organisationseinheit und darunter.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sitzungen

Jul 08, 2016

Das Erhalten der Sitzungsaktivität ist wichtig, um eine optimale Benutzererfahrung zu gewährleisten. Eine Unterbrechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten kann zu Frustrationen bei den Benutzern führen. Ein schneller Wechsel zwischen Arbeitsstationen und Zugriff auf dieselben Anwendungen bei jeder Anmeldung ist eine Priorität für viele mobile Mitarbeiter, z. B. von Mitarbeitern in einem Krankenhaus.

Die folgenden Features dienen dazu, die Sitzungszuverlässigkeit zu optimieren, Unannehmlichkeiten, Ausfallzeiten und Produktivitätsverluste zu reduzieren, und mobilen Benutzern einen schnellen und einfachen Wechsel zwischen Geräten zu ermöglichen.

- Sitzungszuverlässigkeit
- Automatische Wiederverbindung von Clients
- ICA-Keep-Alive
- Workspace Control
- Sitzungsroaming

Im Abschnitt Anmeldeintervall wird beschrieben, wie Sie die Standardeinstellung ändern.

Sie können Benutzer von einer Sitzung abmelden, Sitzungen trennen und Sitzungsvorabstart sowie Sitzungsfortbestehen konfigurieren. Informationen hierzu finden Sie im Artikel Verwalten von Sitzungen über Bereitstellungsgruppen.

# Sitzungszuverlässigkeit

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkkonnektivität unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Diese Funktion ist besonders für mobile Benutzer mit drahtlosen Verbindungen geeignet. Ein Benutzer mit einer drahtlosen Verbindung fährt z. B. in einen Tunnel und die Verbindung wird vorübergehend unterbrochen. Normalerweise würde die Sitzung getrennt und nicht mehr auf dem Bildschirm angezeigt. Der Benutzer müsste sich neu mit der getrennten Sitzung verbinden. Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf der Maschine aktiv. Der Verlust der Verbindung ist zu erkennen, da auf dem Client der Bildschirm fixiert und der Mauszeiger als sich drehende Sanduhr angezeigt wird, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Citrix Receiver-Benutzer können die Controllereinstellung nicht überschreiben.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden. Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und NetScaler Gateway gesendet werden.

Sie aktivieren und konfigurieren die Sitzungszuverlässigkeit mit den folgenden Einstellungen:

- Mit der Richtlinieneinstellung "Sitzungszuverlässigkeit - Verbindungen" können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Der Standardwert für die Einstellung "Sitzungszuverlässigkeit - Timeout" ist 180 Sekunden (3 Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Benutzer nicht zu einer Neuauthentifizierung auffordert, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.
- Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer" geändert.
- Verwenden Sie die Funktion zur automatischen Wiederverbindung von Clients, wenn Sie möchten, dass Benutzer eine Verbindung mit unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können. Sie können die Einstellung für die Citrix Richtlinie "Authentifizierung bei automatischer Wiederverbindung von Clients" so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wiederverbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option "Sitzungszuverlässigkeit - Timeout" festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

# Automatische Wiederverbindung von Clients

Mit der automatischen Wiederverbindung von Clients kann Citrix Receiver unabsichtlich getrennte ICA-Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden. Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können.

Bei Anwendungssitzungen versucht Citrix Receiver, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Desktopsitzungen versucht Citrix Receiver eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;

wobei <*Sekunden*> die Zeit in Sekunden ist, nach deren Ablauf keine weiteren Versuche der Sitzungswiederherstellung erfolgen.

Sie aktivieren und konfigurieren die automatische Wiederverbindung von Clients mit den folgenden Einstellungen:

- **Automatische Wiederverbindung von Clients**: Aktiviert oder deaktiviert die automatische Wiederverbindung desselben Clients, nach dem die Verbindung unterbrochen wurde.
- **Authentifizierung bei automatischer Wiederverbindung von Clients**: Aktiviert oder deaktiviert die erforderliche Benutzerauthentifizierung bei der automatischen Wiederverbindung
- **Protokollierung der automatischen Wiederverbindung von Clients**: Aktiviert oder deaktiviert die Protokollierung von Wiederverbindungsereignissen im Ereignisprotokoll. Die Protokollierung ist standardmäßig deaktiviert. Wenn diese Einstellung aktiviert ist, werden Informationen zu erfolgreichen oder fehlgeschlagenen automatischen Wiederverbindungsereignissen im Systemprotokoll des Servers aufgezeichnet. Jeder Server speichert die Informationen zu Wiederverbindungsereignissen im eigenen Systemprotokoll; die Site stellt kein Protokoll aller Wiederverbindungsereignisse

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

aller Server bereit.

Bei der automatischen Wiederverbindung von Clients findet eine Authentifizierung mit verschlüsselten Anmeldeinformationen statt. Wenn sich ein Benutzer anmeldet, verschlüsselt und speichert der Server die Anmeldeinformationen und erstellt und sendet ein Cookie mit einem Verschlüsselungsschlüssel an Citrix Receiver. Citrix Receiver übergibt den Schlüssel zum Wiederverbinden an den Server. Der Server entschlüsselt die Anmeldeinformationen und gibt sie an die Windows-Anmeldung für eine Authentifizierung weiter. Benutzer müssen sich beim Ablaufen von Cookies neu authentifizieren, um Sitzungen wiederherzustellen.

Cookies werden nicht verwendet, wenn Sie die Einstellung "Authentifizierung bei automatischer Wiederverbindung von Clients" aktivieren. Stattdessen wird der Benutzer in einem Dialogfeld zur Eingabe der Anmeldeinformationen aufgefordert, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.

Zum maximalen Schutz der Anmeldeinformationen von Benutzern und von Sitzungen verwenden Sie die Verschlüsselung für die gesamte Kommunikation zwischen Clients und Site.

Sie deaktivieren die automatische Wiederverbindung in Citrix Receiver für Windows mit der Datei icaclient.adm. Diese Datei liegt derzeit nur in Englisch vor. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Version von Citrix Receiver für Windows.

Einstellungen für Verbindungen wirken sich auch auf die automatische Wiederverbindung von Clients aus:

- In der Standardeinstellung wird die automatische Wiederverbindung von Clients durch Richtlinieneinstellungen auf der Siteebene aktiviert (siehe oben). Der Benutzer muss sich nicht authentifizieren. Wenn jedoch die ICA-TCP-Verbindung eines Servers so konfiguriert wurde, dass Sitzungen mit einer unterbrochenen Kommunikationsverbindung zurückgesetzt werden, findet die automatische Wiederverbindung nicht statt. Die automatische Wiederverbindung von Clients funktioniert nur, wenn der Server Sitzungen trennt, wenn eine unterbrochene Verbindung oder eine Verbindungstimeout vorliegt. In diesem Zusammenhang verweist "ICA-TCP-Verbindung" auf den virtuellen Serverport (nicht auf eine tatsächliche Netzwerkverbindung), der für Sitzungen in TCP/IP-Netzwerken verwendet wird.
- Standardmäßig ist die ICA-TCP-Verbindung auf einem Server so eingestellt, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen, die das Zeitlimit überschritten haben, getrennt werden. Getrennte Sitzungen bleiben im Systemspeicher intakt und stehen für eine Wiederverbindung durch Citrix Receiver zur Verfügung.
- Die Verbindung kann so konfiguriert werden, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen mit Timeouts zurückgesetzt oder abgemeldet werden. Wenn eine Sitzung zurückgesetzt wird, wird bei einem Wiederverbindungsversuch eine neue Sitzung eingeleitet; die Umgebung des Benutzers wird in der verwendeten Anwendung nicht wiederhergestellt, sondern die Anwendung wird neu gestartet.
- Wenn der Server für das Zurücksetzen von Sitzungen konfiguriert ist, erstellt die automatische Wiederverbindung von Clients eine neue Sitzung. Benutzer müssen dann ihre Anmeldeinformationen eingeben, um sich am Server anzumelden.
- Die automatische Wiederverbindung kann fehlschlagen, wenn Citrix Receiver oder das Plug-In falsche Authentifizierungsinformationen übergibt (dies kann während eines Angriffs passieren), oder wenn der Server feststellt, dass zu viel Zeit seit dem Erkennen der unterbrochenen Verbindung verstrichen ist.

# ICA-Keep-Alive

ICA-Keep-Alive verhindert, dass Sitzungen durch unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität erkennt (z. B. keine Zeitänderungen, Mausbewegungen oder Bildschirmaktualisierungen) wird verhindert, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Pakete, um zu


© 1999-2017 Citrix Systems, Inc. All rights reserved.

erkennen, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

**Hinweis:** ICA-Keep-Alive funktioniert nur, wenn Sie die Sitzungszuverlässigkeit nicht verwenden. Die Sitzungszuverlässigkeit hat eigene Mechanismen für das Aufrechterhalten von Verbindungen. Konfigurieren Sie ICA-Keep-Alive nur für Verbindungen, die keine Sitzungszuverlässigkeit verwenden.

ICA-Keep-Alive-Einstellungen überschreiben Keep-Alive-Einstellungen, die für Microsoft Windows-Gruppenrichtlinien konfiguriert wurden.

Sie aktivieren und konfigurieren ICA-Keep-Alive mit den folgenden Einstellungen:

- **ICA-Keep-Alive - Timeout**: Gibt das Intervall (1-3600 Sekunden) für das Senden von ICA-Keep-Alive-Meldungen an. Konfigurieren Sie diese Option nicht, wenn die Netzwerksoftware inaktive Sitzungen schließen soll und unterbrochene Verbindungen in der Umgebung so selten sind, dass die Wiederverbindung mit Sitzungen nicht wichtig ist.
  Die Standardeinstellung von 60 Sekunden bedeutet, dass alle 60 Sekunden ICA-Keep-Alive-Pakete an Benutzergeräte gesendet werden. Antwortet ein Benutzergerät nicht in 60 Sekunden, wird der Status der ICA-Verbindung auf "Getrennt" gesetzt.
- **ICA-Keep-Alives**: Sendet oder verhindert das Senden von ICA-Keep-Alive-Meldungen.

# Workspace Control

Mit Workspace Control können Desktops und Anwendungen einem Benutzer von einem Gerät zum anderen folgen. Diese Roamingfähigkeit ermöglicht Benutzern den Zugriff auf alle Desktops oder offene Anwendungen von einem beliebigen Ort aus, ohne Neustart des Desktops oder der Anwendungen auf jedem einzelnen Gerät. Sie müssen sich lediglich anmelden. Mit Workspace Control kann das Pflegepersonal in einem Krankenhaus beispielsweise schnell an eine andere Arbeitsstation wechseln und nach der Anmeldung auf dieselben Anwendungen zugreifen. Bei entsprechender Konfiguration von Workspace Control können die Mitarbeiter die Verbindung zu mehreren Anwendungen auf einem Clientgerät trennen und die Verbindung zu denselben Anwendungen auf einem anderen Clientgerät wiederherstellen.

Workspace Control wirkt sich auf die folgenden Aktivitäten aus:

- **Anmelden**: Standardmäßig ermöglicht Workspace Control den Benutzern, die Verbindung mit allen ausgeführten Desktops und Anwendungen bei der Anmeldung automatisch wiederherzustellen, ohne sie erneut manuell zu öffnen. Mit Workspace Control können Benutzer getrennte Desktops oder Anwendungen öffnen sowie alle, die auf einem anderen Clientgerät aktiv sind. Beim Trennen der Verbindung mit einem Desktop bzw. einer Anwendung wird das Desktop bzw. die Anwendung weiterhin auf dem Server ausgeführt. Bei Benutzern im Roamingbetrieb, die einige Desktops oder Anwendungen auf einem Clientgerät ausführen müssen, während sie auf einem anderen Clientgerät eine Wiederverbindung zu einem Teil ihres Desktops bzw. ihrer Anwendungen durchführen möchten, können Sie das Wiederverbindungsverhalten bei der Anmeldung so konfigurieren, dass nur die Desktops bzw. Anwendungen geöffnet werden, die zuvor getrennt wurden.
- **Wiederverbinden**: Nach der Anmeldung beim Server können Benutzer eine Verbindung zu all ihren Desktops oder Anwendungen jederzeit wiederherstellen, indem Sie auf "Wiederverbinden" klicken. Beim Wiederverbinden werden standardmäßig sowohl getrennte Desktops oder Anwendungen geöffnet als auch alle aktiven Anwendungen, die derzeit auf einem anderen Clientgerät ausgeführt werden. Sie können die Wiederverbindung so konfigurieren, dass nur die Desktops oder Anwendungen geöffnet werden, deren Verbindung der Benutzer zuvor getrennt hat.
- **Abmelden**: Bei Benutzern, die Desktops oder Anwendungen über StoreFront öffnen, können Sie den Abmeldebefehl so

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

konfigurieren, dass Benutzer entweder von StoreFront und allen aktiven Sitzungen gleichzeitig oder nur von StoreFront abgemeldet werden.
- **Verbindung wird getrennt**: Benutzer können die Verbindung mit allen ausgeführten Desktops und Anwendungen gleichzeitig trennen.

Workspace Control ist nur für Benutzer von Citrix Receiver verfügbar, die über eine Citrix StoreFront-Verbindung auf Desktops und Anwendungen zugreifen. Workspace Control ist standardmäßig für virtuelle Desktopsitzungen deaktiviert, für gehostete Anwendungen aber aktiviert. Die Sitzungsfreigabe zwischen veröffentlichten Desktops und veröffentlichten Anwendungen in diesen Desktops erfolgt nicht standardmäßig.

Benutzerrichtlinien, Clientlaufwerkzuordnungen und Druckerkonfigurationen ändern sich entsprechend, wenn ein Benutzer ein neues Clientgerät verwendet. Diese Richtlinien und Zuordnungen werden auf dem Clientgerät angewendet, auf dem der Client derzeit bei der Sitzung angemeldet ist. Wenn sich Pflegepersonal z. B. von einem Clientgerät in der Notaufnahme des Krankenhauses abmeldet und dann bei einer Arbeitsstation in der Röntgenabteilung anmeldet, gelten für die Sitzung die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen der Röntgenabteilung, solange die Sitzung gestartet wird.

Sie können die den Benutzern angezeigten Drucker je nach Standort anpassen. Außerdem können Sie steuern, ob Benutzer auf lokalen Druckern drucken können, wie viel Bandbreite bei einer Remoteverbindung verwendet wird sowie andere Aspekte des Druckens.

Weitere Informationen zur Aktivierung und Konfiguration von Workspace Control für Benutzer finden Sie in der StoreFront-Dokumentation.

# Sitzungsroaming

Standardmäßig wechseln Sitzungen zusammen mit dem Benutzer von Clientgerät zu Clientgerät. Wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet, wird die gleiche Sitzung verwendet und die Anwendungen stehen auf beiden Geräten zur Verfügung. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. In vielen Fällen folgen auch Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind.

Dieses Standardverhalten bietet viele Vorteile, ist aber nicht in allen Fällen ideal. Sie können das Sitzungsroaming mit dem PowerShell-SDK verhindern.

Beispiel 1: Ein Mitarbeiter eines Krankenhauses verwendet beim Ausfüllen eines Versicherungsformulars einen Desktop-PC und ein Tablet zum Anzeigen von Patientendaten.

- Bei aktiviertem Sitzungsroaming werden beide Anwendungen auf beiden Geräten angezeigt (eine auf einem Gerät gestartete Anwendung ist auf allen Geräten zu sehen). Dies entspricht möglicherweise nicht den Sicherheitsanforderungen.
- Wenn das Sitzungsroaming deaktiviert ist, werden die Patientendaten nicht auf dem PC angezeigt und das Versicherungsformular nicht auf dem Tablet.

Beispiel 2: Ein Produktionsmanager startet eine Anwendung auf dem PC im Büro. Gerätename und Standort bestimmen, welche Drucker und anderen Ressourcen für die Sitzung verfügbar sind. Später nimmt er bei einer Besprechung in einem anderen Gebäude teil und muss etwas ausdrucken.

- Bei aktiviertem Sitzungsroaming kann er wahrscheinlich nicht auf die Drucker in der Nähe des Besprechungsraums zugreifen, da ihm durch den Anwendungsstart Drucker und Ressourcen für den Standort Büro zugewiesen wurden.

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

- Ist das Sitzungsroaming deaktiviert, wird bei der Anmeldung bei einem anderen Gerät (mit denselben Anmeldeinformationen) eine neue Sitzung gestartet und Drucker und Ressourcen in der Nähe werden verfügbar.

## Konfigurieren des Sitzungsroamings

Zum Konfigurieren des Sitzungsroamings verwenden Sie die folgenden Anspruchsrichtlinienregel-Cmdlets mit der Eigenschaft "SessionReconnection". Optional können Sie auch die Eigenschaft "LeasingBehavior" festlegen. Weitere Informationen finden Sie weiter unten unter "Verbindungsleasing und Sitzungsroaming".

Desktopsitzungen:

> Set-BrokerEntitlementPolicyRule <*Name der Bereitstellungsgruppe*> -SessionReconnection <*Wert*> -LeasingBehavior Allowed|Disallowed

Anwendungssitzungen:

> Set-BrokerAppEntitlementPolicyRule <*Name der Bereitstellungsgruppe*> -SessionReconnection <*Wert*> -LeasingBehavior Allowed|Disallowed

<*Wert*> kann einer der folgenden Werte sein:

- **Always**: Das Sitzungsroaming ist immer aktiviert, unabhängig vom Clientgerät und davon, ob die Sitzung verbunden oder getrennt ist. Dies ist der Standardwert.
- **DisconnectedOnly**: Eine Wiederverbindung erfolgt nur bei Sitzungen, die bereits getrennt sind. Andernfalls wird eine neue Sitzung gestartet. (Sitzungen können zwischen Clientgeräten wechseln, indem sie zunächst getrennt werden oder das Roaming für sie explizit mit Workspace Control durchgeführt wird.) Eine aktive verbundene Sitzung von einem anderen Clientgerät wird nie verwendet, stattdessen wird eine neue Sitzung gestartet.
- **SameEndpointOnly**: Der Benutzer erhält eine eigene Sitzung für jedes verwendete Clientgerät. Damit wird das Sitzungsroaming vollständig deaktiviert. Die Benutzer können eine Wiederverbindung nur auf dem Gerät vornehmen, das zuvor für die Sitzung verwendet wurde.

Die Eigenschaft "LeasingBehavior" wird weiter unten beschrieben.

**Auswirkungen anderer Einstellungen**

Das in den Anwendungseigenschaften einer Bereitstellungsgruppe über "Nur eine Anwendungsinstanz pro Benutzer zulassen" festgelegte Anwendungslimit hat Auswirkungen auf die Deaktivierung des Sitzungsroamings.

- Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch die Option "Nur eine Anwendungsinstanz pro Benutzer zulassen".
- Wenn Sie die Option "Nur eine Anwendungsinstanz pro Benutzer zulassen" aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden.

## Verbindungsleasing und Sitzungsroaming

Wenn Sie nicht mit dem Verbindungsleasing vertraut sind, lesen Sie den Artikel Verbindungsleasing.

Wenn ein Controller auf eine geleaste Verbindung schaltet, tritt für die Sitzungswiederverbindung wieder der Standardwert in Kraft, d. h. die Wiederverbindung erfolgt nur mit einer aktiven oder getrennten Sitzung für den Desktop bzw. die Anwendung.

Zur Gewährleistung zusätzlicher Sicherheit sollten Sie, wenn Sie für das Sitzungsroaming einen anderen als den

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Standardwert konfiguriert haben und mehrere Benutzer auf mehreren Geräten dieselben Anmeldeinformationen verwenden, das Verbindungsleasing für die Bereitstellungsgruppe, die das verwendete Benutzerkonto enthält, deaktivieren.

Erklärung In diesem Szenario wird eine Sitzung auf allen Geräten gemeinsam verwendet. Das ist möglicherweise unerwünscht, z. B. wenn ein Benutzer vertrauliche Informationen anzeigt, die andere Benutzer, die sich mit denselben Anmeldeinformationen wieder verbinden, während der Controller im Leasingverbindungsmodus ausgeführt wird, nicht sehen sollen.

Durch Deaktivieren des Verbindungsleasings in der Anspruchsrichtlinie wird dies verhindert, d. h. Benutzer können die Sitzung anderer mit den gleichen Anmeldeinformationen angemeldeter Benutzer nicht sehen, selbst wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Andere Anspruchsrichtlinien können bestehen bleiben; einzelne Benutzerkonten können das Verbindungsleasing über separate Ansprüche nutzen.

Zum Deaktivieren des Verbindungsleasings in einer Anspruchrichtlinie fügen Sie die Eigenschaft "LeasingBehavior Disallowed" dem Cmdlet der Anspruchsrichtlinie hinzu. Wenn Sie das Verbindungsleasing deaktivieren, müssen Sie alle für die Anspruchsrichtlinie bereits erstellten und zwischengespeicherten Startleases manuell löschen. Andernfalls können sich die Benutzer nach wie vor wieder verbinden, wenn es zum Ausfall der Datenbank kommt.

# Anmeldeintervall

Wenn eine virtuelle Maschine mit einem Desktop-VDA geschlossen wird, bevor die Anmeldung abgeschlossen ist, können Sie dem Prozess mehr Zeit zuteilen. Die Standardeinstellung in Version 7.6 und höher ist 180 Sekunden (die Standardeinstellung für Version 7.0-7.5 ist 90 Sekunden).

Legen Sie auf der Maschine (oder dem im Maschinenkatalog verwendeten Masterimage) folgenden Registrierungsschlüssel fest:

Schlüssel: HKLM\SOFTWARE\Citrix\PortICA

Wert: AutoLogonTimeout

Typ: DWORD

Geben Sie die Zeit als Dezimalwert in Sekunden ein, zulässig ist ein Wert von 0 bis 3600.

Wenn Sie ein Masterimage ändern, aktualisieren Sie den Katalog.

**Hinweis:** Diese Einstellung gilt nur für VMs mit Desktop-VDAs, das Anmeldetimeout auf Server-VDAs wird von Microsoft gesteuert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwenden der Suche in Studio

Jul 08, 2016

Verwenden Sie die Suchfunktion, um Informationen zu spezifischen Maschinen, Sitzungen, Maschinenkatalogen, Anwendungen oder Bereitstellungsgruppen zu finden.

1. Wählen Sie im Studio-Navigationsbereich Suchen aus.
   Hinweis: Sie können mit dem Suchfeld der Registerkarten "Maschinenkataloge" oder "Bereitstellungsgruppen" keine Suche durchführen. Verwenden Sie den Suchknoten im Navigationsbereich.
   Zum Anzeigen weiterer Suchkriterien klicken Sie auf das Pluszeichen neben den Dropdownlisten. Klicken Sie zum Entfernen von Suchkriterien auf das Minuszeichen.

2. Geben Sie den Namen ein oder verwenden Sie die Dropdownliste, um eine andere Suchoption für das gesuchte Element auszuwählen.
3. Speichern Sie Ihre Suche, falls gewünscht, durch Wählen von Speichern unter. Die Suche wird in der Liste "Gespeicherte Suchvorgänge" angezeigt.

Sie können auch auf das Symbol "Suche erweitern" (doppelte nach unten gerichtete spitze Klammern) klicken, um eine Dropdownliste mit Sucheigenschaften anzuzeigen. Führen Sie eine erweiterte Suche durch, indem Sie einen Ausdruck anhand der Eigenschaften in der Dropdownliste zusammenstellen.

Tipps zur Verbesserung der Suche:

- Um zusätzliche Eigenschaften in die Anzeige zu integrieren, anhand derer Sie dann suchen und sortieren können, klicken Sie mit der rechten Maustaste auf eine Spalte und wählen Sie Spalten auswählen.
- Wählen Sie zum Suchen eines mit einer Maschine verbundenen Benutzergeräts "Client (IP)" und "ist", und geben Sie die IP-Adresse des Geräts ein.
- Wenn Sie aktive Sitzungen suchen, verwenden Sie "Sitzungszustand", "ist" und "Verbunden".
- Um alle Maschinen in einer Bereitstellungsgruppe aufzuführen, wählen Sie im Navigationsbereich Bereitstellungsgruppen, wählen Sie die Gruppe aus und wählen Sie dann im Aktionsbereich Maschinen anzeigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Tags

Jul 08, 2016

Tags sind Zeichenfolgen zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Bereitstellungsgruppen und Richtlinien. Durch Erstellen und Hinzufügen von Tags können Sie festlegen, dass bestimmte Vorgänge nur an Elementen stattfinden, die ein spezifisches Tag haben.

- Anpassen der Suchanzeige in Studio

  Wenn Sie beispielsweise nur Anwendungen anzeigen möchten, die für Testzwecke optimiert wurden, fügen den Anwendungen ein Tag mit dem Namen "Test" hinzu. Filtern Sie dann die Suche in Studio nach dem Tag "Test". Oder wenn Sie nur Bereitstellungsgruppen anzeigen möchten, die Mitglieder des Testteams enthalten, fügen Sie den betreffenden Bereitstellungsgruppen das Tag "Testteam" hinzu und filtern Sie die Suche in Studio nach diesem Tag.

- Zuweisen von Citrix Richtlinien auf Anwendungen, Maschinen oder Bereitstellungsgruppen mit (oder ohne) einem bestimmten Tag

  Wenn Sie beispielsweise eine Citrix Richtlinie nur auf leistungsstarke Arbeitsstationen anwenden möchten, fügen Sie diesen Maschinen ein Tag mit dem Namen "Hohe Leistung" hinzu. Wählen Sie dann auf der Zuweisungsseite des Assistenten zum Erstellen von Richtlinien dieses Tag und das Kontrollkästchen zum Aktivieren. Sie können auch einer Bereitstellungsgruppe ein Tag hinzufügen und eine Citrix Richtlinie auf die Gruppe anwenden.

# Verwalten von Tags

Wählen Sie in Studio eine Maschine, Anwendung oder Bereitstellungsgruppe und dann im Aktionsbereich **Tags verwalten**. Das Dialogfeld "Tags verwalten" enthält alle in der Site erstellten Tags und nicht nur diejenigen, die für das ausgewählte Element erstellt wurden.

- Ist das Kontrollkästchen eines Tags aktiviert, wurde das Tag dem ausgewählten Element bereits hinzugefügt.
- Wenn Sie eine Bereitstellungsgruppe auswählen, wird durch ein Kontrollkästchen mit einem Bindestrich angezeigt, wenn einigen (aber nicht allen) Elementen in der Gruppe Tags hinzugefügt wurden.

Die folgenden Aktionen stehen im Dialogfeld "Tags verwalten" zur Verfügung:

- Zum Hinzufügen oder Entfernen von Tags aktivieren oder deaktivieren Sie das zugehörige Kontrollkästchen.
- Zum Erstellen eins Tags wählen Sie **Tag erstellen**. Geben Sie einen Namen und eine Beschreibung ein. Tagnamen müssen eindeutig sein, die Groß- und Kleinschreibung spielt keine Rolle. Klicken Sie dann auf **OK**.
- Zum Bearbeiten eines Tags wählen Sie das Tag und dann **Tag bearbeiten**. Ändern Sie den Namen und/oder die Beschreibung und klicken Sie dann auf **Speichern**. Sie können immer nur ein Tag bearbeiten.
- Zum Löschen eines oder mehrerer Tags wählen Sie die Tags und dann **Tag löschen**. Im Dialogfeld "Tag löschen" wird angezeigt, von wie vielen Elementen die ausgewählten Tags verwendet werden. Klicken Sie zum Anzeigen weiterer Informationen auf ein Element. Sind beispielsweise zwei Maschinen betroffen, werden durch Klicken auf das Element die beiden Maschinennamen angezeigt. Nach dem Prüfen der betroffenen Elemente bestätigen Sie, ob Sie die Tags löschen möchten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Unterstützung für IPv4/IPv6

Jul 08, 2016

Dieses Release unterstützt reines IPv4, reines IPv6 und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden.

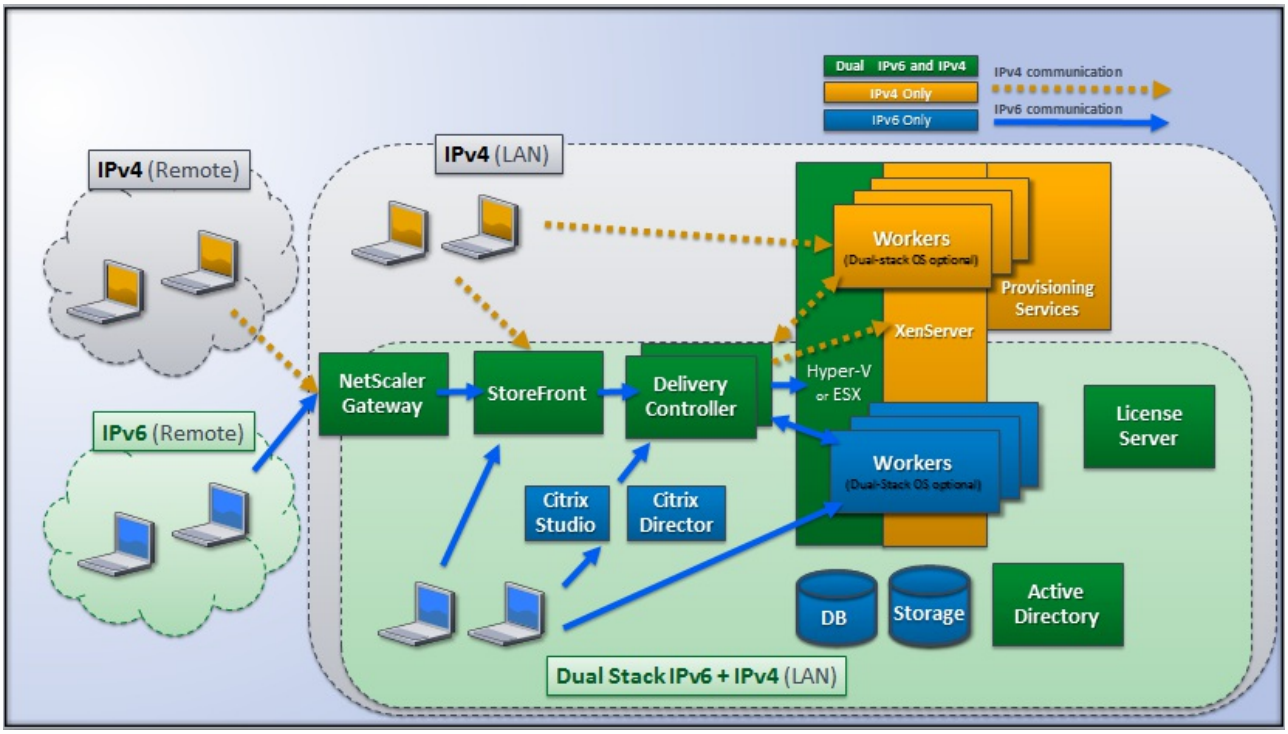
Die IPv6-Kommunikation wird mit zwei verbindungsspezifischen Citrix Richtlinieneinstellungen für Virtual Delivery Agent (VDA) gesteuert:

- Die primäre Einstellung erzwingt die Verwendung von IPv6: Nur IPv6-Controllerregistrierung verwenden.
- Die abhängige Einstellung definiert eine IPv6-Netzwerkmaske: IPv6-Netzwerkmaske für Controllerregistrierung.

Wenn Nur IPv6-Controllerregistrierung verwenden aktiviert ist, erfolgt die VDA-Registrierung bei einem Delivery Controller für eingehende Verbindungen über eine IPv6-Adresse.

## IPv4-/IPv6-Bereitstellung mit dualem Stapel

Die folgende Abbildung zeigt eine IPv4-/IPv6-Bereitstellung mit dualem Stapel. In diesem Szenario ist ein Worker ein auf einem Hypervisor oder auf einer physischen Maschine installierter VDA, der primär zum Aktivieren von Verbindungen für Anwendungen und Desktops verwendet wird. Komponenten, die für den Parallelbetrieb von IPv6 und IPv4 ausgelegt sind, werden auf Betriebssystemen ausgeführt, die Tunneling oder Dual Protocol-Software nutzen.




Diese Citrix Produkte, Komponenten und Features unterstützen nur IPv4:

- Provisioning Services
- XenServer Version 6.x
- VDAs, die nicht mit der Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** gesteuert werden
- XenApp-Versionen vor 7.5, XenDesktop-Versionen vor 7 und Director

In dieser Bereitstellung gilt:

- Wenn ein Team häufig ein IPv6-Netzwerk verwendet und der Administrator die Nutzung von IPv6-Datenverkehr


© 1999-2017 Citrix Systems, Inc. All rights reserved.

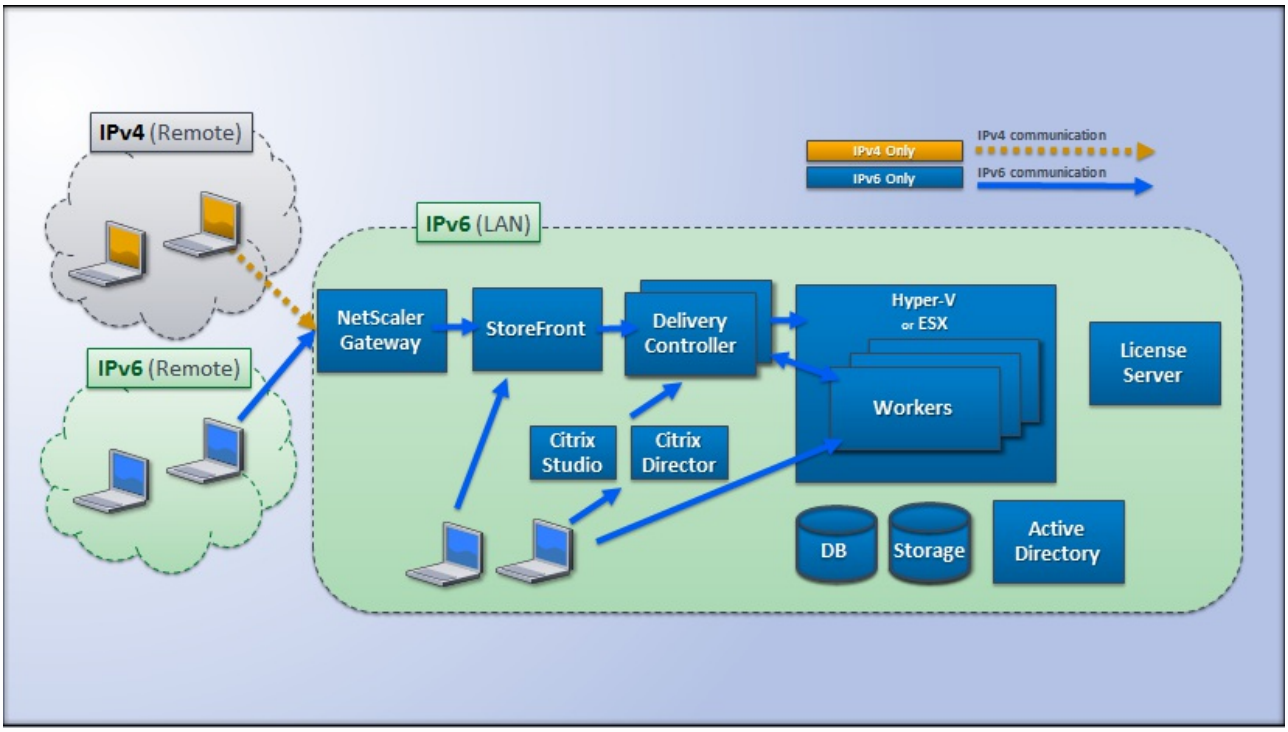
wünscht, veröffentlicht der Administrator IPv6-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) aktiviert ist.

- Wenn ein Team häufig ein IPv4-Netzwerk verwendet, veröffentlicht der Administrator IPv4-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung deaktiviert ist (d. h. Nur IPv6-Controllerregistrierung verwenden ist deaktiviert = Standardeinstellung).

### Reine IPv6-Bereitstellung

Die folgende Abbildung zeigt eine reine IPv6-Bereitstellung. Für dieses Szenario gilt:

- Die Komponenten werden auf Betriebssystemen ausgeführt, die ein IPv6-Netzwerk unterstützen.
- Die primäre Citrix Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) ist für alle VDAs aktiviert; sie müssen sich beim Controller mit einer IPv6-Adresse registrieren.




## Richtlinieneinstellungen für IPv6

Bei reiner IPv6-Implementierung bzw. Implementierung von IPv4/IPv6 mit dualem Stapel sind zwei Citrix Richtlinieneinstellungen relevant. Konfigurieren Sie die folgenden verbindungsbezogenen Einstellungen:

- **Nur IPv6 Controllerregistrierung verwenden**: steuert das Adressformat, mit dem der Virtual Delivery Agent (VDA) beim Delivery Controller registriert wird. Standard = deaktiviert
  - Wenn der VDA mit dem Controller kommuniziert, wird eine IPv6-Adresse verwendet, deren Auswahl folgender Reihenfolge unterliegt: globale IP-Adresse, Unique Local Address (ULA), Link-Local-Adresse (nur wenn keine anderen IPv6-Adressen verfügbar sind).
  - Bei deaktivierter Einstellung wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.
- **IPv6-Netzwerkmaske für Controllerregistrierung**: Eine Maschine kann über mehrere IPv6-Adressen verfügen. Mit dieser Richtlinieneinstellung können Administratoren den VDA auf ein bevorzugtes Subnetz beschränken (anstelle einer globalen IP, sofern registriert). Mit dieser Einstellung wird das Netzwerk festgelegt, in dem der VDA registriert wird: Der VDA wird nur bei der ersten Adresse registriert, die mit der angegebenen Netzwerkmaske übereinstimmt. Diese


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Einstellung ist nur gültig, wenn die Richtlinieneinstellung Nur IPv6-Controllerregistrierung verwenden aktiviert ist. Standard = leere Zeichenfolge

**Wichtig:** Die Verwendung von IPv4 oder IPv6 durch einen VDA wird ausschließlich über diese Richtlinieneinstellungen gesteuert. Das bedeutet, um die IPv6-Adressierung nutzen zu können, muss der VDA von einer Citrix Richtlinie gesteuert werden, bei der die Einstellung **Nur IPv6-Controllerregistrierung verwenden** aktiviert ist.

## Überlegungen zur Bereitstellung

Wenn Ihre Umgebung sowohl IPv4- und IPv6-Netzwerke umfasst, benötigen Sie separate Bereitstellungsgruppenkonfigurationen für IPv4-exklusive Clients und für die Clients, die Zugriff auf das IPv6-Netzwerk haben. Verwenden Sie ggf. Namen, die manuelle Active Directory-Gruppenzuweisung oder SmartAccess-Filter zur Unterscheidung der Benutzer.

Die Wiederverbindung mit einer Sitzung kann fehlschlagen, wenn die Verbindung auf einem IPv6-Netzwerk initiiert wird und dann Wiederverbindungsversuche von einem internen Client erfolgen, der nur über IPv4-Zugriff verfügt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Clientordnerumleitung

Jul 08, 2016

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner statt des kompletten Dateisystems auf dem Benutzergerät werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt.

Die Clientordnerumleitung wird nur auf Windows-Desktopbetriebssystemmaschinen unterstützt.

Die Clientordnerumleitung für ein externes USB-Laufwerk wird beim Trennen und Wiederverbinden des Geräts nicht gespeichert.

Aktivieren Sie die Clientordnerumleitung auf dem Server. Geben Sie dann auf dem Clientgerät an, welche Ordner umgeleitet werden sollen (die Anwendung, die Sie zur Angabe der Clientordneroptionen verwenden, ist in diesem Release von Citrix Receiver enthalten).

**Achtung:** Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Auf dem Server:
   1. Erstellen Sie einen Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
   2. Erstellen Sie einen Wert für REG_DWORD.
      - Name: CFROnlyModeAvailable
      - Typ: REG_DWORD
      - Wert: Stellen Sie 1 ein.
2. Auf dem Benutzergerät:
   1. Stellen Sie sicher, dass die neueste Version von Citrix Receiver installiert ist.
   2. Starten Sie vom Installationsverzeichnis von Citrix Receiver aus CtxCFRUI.exe.
   3. Wählen Sie das Optionsfeld Benutzerdefiniert und fügen Sie Ordner hinzu oder bearbeiten oder entfernen Sie Ordner.
   4. Trennen Sie die Sitzungen und stellen Sie dann neue Verbindungen her, damit die Einstellung wirksam wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Benutzerprofile

Jul 08, 2016

Standardmäßig wird bei der Installation des Virtual Delivery Agents die Citrix Profilverwaltung ohne Benutzereingriff auf Masterimages installiert. Sie muss jedoch nicht als Profillösung verwendet werden.

Mit XenApp- und XenDesktop-Richtlinien können Sie auf die Maschinen jeder Bereitstellungsgruppe ein anderes Profilverhalten anwenden, um die Profile an unterschiedliche Benutzerbedürfnisse anzupassen. Beispiel: Eine Bereitstellungsgruppe erfordert möglicherweise verbindliche Citrix Profile, deren Vorlage an einem Netzwerkspeicherort gespeichert ist, aber eine andere Bereitstellungsgruppe erfordert möglicherweise Citrix Roamingprofile an einem anderen Speicherort mit mehreren umgeleiteten Ordnern.

- Wenn andere Administratoren in Ihrer Organisation für XenApp- und XenDesktop-Richtlinien zuständig sind, stimmen Sie gemeinsam ab, welche profilbezogenen Richtlinien für die Bereitstellungsgruppen gelten.
- Richtlinien zur Profilverwaltung können auch in der Gruppenrichtlinie sowie in der INI-Datei der Profilverwaltung und lokal auf einzelnen virtuellen Maschinen festgelegt werden. Diese verschiedenen Methoden zum Definieren des Profilverhaltens werden in der folgenden Reihenfolge gelesen:
  1. Gruppenrichtlinie (ADM- oder ADMX-Dateien)
  2. XenApp- und XenDesktop-Richtlinien im Knoten "Richtlinie"
  3. Lokale Richtlinien auf der virtuellen Maschine, zu der der Benutzer eine Verbindung herstellt
  4. INI-Datei der Profilverwaltung

  Beispiel: Wenn Sie die gleiche Richtlinie sowohl in der Gruppenrichtlinie als auch im Knoten "Richtlinie" konfigurieren, wird die Richtlinieneinstellung in der Gruppenrichtlinie vom System gelesen und die XenApp- bzw. XenDesktop-Richtlinieneinstellung wird ignoriert.

Unabhängig davon, für welche Lösung Sie sich entscheiden, können Director-Administratoren auf Diagnoseinformationen zugreifen und Problembehandlung für Benutzerprofile durchführen. Weitere Informationen finden Sie in der Dokumentation für Director.

Wenn Sie das Personal vDisk-Feature verwenden, werden Citrix Benutzerprofile standardmäßig auf den persönlichen vDisks der virtuellen Desktops gespeichert. Löschen Sie die Kopie eines Profils im Benutzerspeicher nicht, wenn gleichzeitig eine Kopie auf der persönlichen vDisk verbleibt. Dies würde einen Profilverwaltungsfehler auslösen und dazu führen, dass für Anmeldungen an dem virtuellen Desktop ein temporäres Profil verwendet wird.

## Automatische Konfiguration

Der Desktoptyp wird automatisch basierend auf der VDA-Installation erkannt und entsprechende Standardwerte für die Profilverwaltung werden neben Ihrer Konfigurationsauswahl in Studio festgelegt.

Die Richtlinien, die von der Profilverwaltung angepasst werden, werden in der Tabelle unten angezeigt. Nicht-Standard-Richtlinieneinstellungen bleiben erhalten und werden nicht von diesem Feature überschrieben. Weitere Informationen zu jeder Richtlinie finden Sie in der Dokumentation zur Profilverwaltung. Die Maschinentypen, für die Profile erstellt werden, wirken sich auf die angepassten Richtlinien aus. Wichtig ist, ob Maschinen persistent oder bereitgestellt sind, und ob sie von mehreren Benutzern gemeinsam verwendet werden oder nur einem dedizierten Benutzer zugeordnet sind.

Persistente Systeme verfügen über einen lokalen Speicher, dessen Inhalt auch nach dem Abschalten des Systems bestehen bleibt. Persistente Systeme imitieren u. U. mit Speichertechnologien wie Speichernetzwerke (Storage Area Networks, SANs) einen lokalen Datenträger. Bereitgestellte Systeme werden dagegen bei Bedarf von einem Basisdatenträger und einem Identitätsdatenträger erstellt. Der lokale Speicher wird üblicherweise durch eine RAM-Disk oder Netzwerk-Disk imitiert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Letztere wird oft über ein SAN mit einer Hochgeschwindigkeitsverbindung zur Verfügung gestellt. Für die Bereitstellung wird allgemein Provisioning Services oder die Maschinenerstellungsdienste (oder ein entsprechendes Produkt eines Drittanbieters) verwendet. Manchmal haben bereitgestellte Systeme persistenten lokalen Speicher, der möglicherweise durch persönliche vDisks zur Verfügung gestellt wird; diese werden als persistent klassifiziert.

Zusammen definieren diese beiden Faktoren die folgenden Maschinentypen:

- **Persistent und dediziert**: Beispiele sind Desktopbetriebssystemmaschinen mit festen Zuweisungen und einer persönlichen vDisk, die mit den Maschinenerstellungsdiensten erstellt wurden, Desktops mit persönlichen vDisks, die in VDI-in-a-Box erstellt wurden, physische Arbeitsstationen und Laptops.
- **Persistent und freigegeben**: Beispiele sind Serverbetriebssystemmaschinen, die mit den Maschinenerstellungsdiensten erstellt wurden.
- **Bereitgestellt und dediziert**: Beispiele sind Desktopbetriebssystemmaschinen mit statischen Zuweisungen, aber ohne persönliche vDisk, die mit Provisioning Services erstellt wurden.
- **Bereitgestellt und freigegeben**: Beispiele sind Desktopbetriebssystemmaschinen mit zufälliger Zuweisung, die mit Provisioning Services erstellt wurden, und Desktops ohne persönliche vDisks, die mit VDI-in-a-Box erstellt wurden.

Die folgenden Richtlinieneinstellungen der Profilverwaltung werden für die verschiedenen Maschinentypen empfohlen. Sie funktionieren in den meisten Fällen gut, aber Sie müssen sie ggf. an die Anforderungen Ihrer Bereitstellung anpassen.

Wichtig: Lokal zwischengespeicherte Profile nach Abmeldung löschen, Profilstreaming und Immer zwischenspeichern werden durch die automatische Konfiguration erzwungen. Passen Sie die anderen Richtlinien manuell an.

**Persistente Maschinen**

| Richtlinie | Persistent und dediziert | Persistent und freigegeben |
|---|---|---|
| Lokal zwischengespeicherte Profile nach Abmeldung löschen | Deaktiviert | Aktiviert |
| Profilstreaming | Deaktiviert | Aktiviert |
| Immer zwischenspeichern | Aktiviert (Hinweis 1) | Deaktiviert (Hinweis 2) |
| Aktiv zurückschreiben | Deaktiviert | Deaktiviert (Hinweis 3) |
| Anmeldungen lokaler Administratoren verarbeiten | Aktiviert | Deaktiviert (Hinweis 4) |

**Bereitgestellte Maschinen**

| Richtlinie | Bereitgestellt und dediziert | Bereitgestellt und freigegeben |
|---|---|---|
| Lokal zwischengespeicherte Profile nach Abmeldung | Deaktiviert (Hinweis 5) | Aktiviert |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Richtlinie | Bereitgestellt und dediziert | Bereitgestellt und freigegeben |
|---|---|---|
| Profilstreaming | Aktiviert | Aktiviert |
| | | |
| Immer zwischenspeichern | Deaktiviert (Hinweis 6) | Deaktiviert |
| Aktiv zurückschreiben | Aktiviert | Aktiviert |
| Anmeldungen lokaler Administratoren verarbeiten | Aktiviert | Aktiviert (Hinweis 7) |

1. Da Profilstreaming für diesen Maschinentyp deaktiviert ist, wird die Einstellung Immer zwischenspeichern immer ignoriert.
2. Deaktivieren Sie Immer zwischenspeichern. Sie können sicherstellen, dass große Dateien möglichst bald nach der Anmeldung in Profile geladen werden, wenn Sie diese Richtlinie aktivieren und mit ihr ein Dateigrößenlimit definieren (in MB). Dateien, die diese Größe überschreiten, werden so schnell wie möglich lokal zwischengespeichert.
3. Deaktivieren Sie Aktiv zurückschreiben, außer wenn Sie Änderungen in Profilen für Benutzer speichern, die zwischen XenApp-Servern roamen. Aktivieren Sie in dieser Situation diese Richtlinie.
4. Deaktivieren Sie Anmeldungen lokaler Administratoren verarbeiten, außer für gehostete, freigegebene Desktops. Aktivieren Sie in dieser Situation diese Richtlinie.
5. Deaktivieren Sie Lokal zwischengespeicherte Profile nach Abmeldung löschen. Damit bleiben lokal zwischengespeicherte Profile erhalten. Da die Maschinen beim Abmelden zurückgesetzt werden, aber einzelnen Benutzern zugewiesen sind, ist die Anmeldung mit zwischengespeicherten Profile schneller.
6. Deaktivieren Sie Immer zwischenspeichern. Sie können sicherstellen, dass große Dateien möglichst bald nach der Anmeldung in Profile geladen werden, wenn Sie diese Richtlinie aktivieren und mit ihr ein Dateigrößenlimit definieren (in MB). Dateien, die diese Größe überschreiten, werden so schnell wie möglich lokal zwischengespeichert.
7. Aktivieren Sie Anmeldungen lokaler Administratoren verarbeiten, außer für Benutzer, die zwischen XenApp- und XenDesktop-Servern roamen. Deaktivieren Sie in dieser Situation diese Richtlinie.

## Ordnerumleitung

Die Ordnerumleitung ermöglicht das Speichern von Benutzerdaten auf Netzwerkfreigaben, die nicht zum Speichern von Profilen verwendet werden. Dies verringert die Profilgröße und die Ladezeit, hat aber möglicherweise Auswirkungen auf die Netzwerkbandbreite. Zur Ordnerumleitung müssen keine Citrix Benutzerprofile verwendet werden. Sie können die Benutzerprofile selbst verwalten und dennoch Ordner umleiten.

Konfigurieren Sie die Ordnerumleitung mit den Citrix Richtlinien in Studio.

- Stellen Sie sicher, dass die Netzwerkspeicherorte zum Speichern des Inhalts von umgeleiteten Ordnern verfügbar sind, und die erforderlichen Berechtigungen richtig sind. Die Speicherorteigenschaften werden überprüft.
- Umgeleitete Ordner werden im Netzwerk eingerichtet und mit Inhalten der virtuellen Desktops bei der Anmeldung aufgefüllt.

Hinweis: Konfigurieren Sie die Ordnerumleitung entweder mit den Citrix Richtlinien oder den Active Directory-Gruppenrichtlinienobjekten, jedoch nicht mit beiden. Das Konfigurieren der Ordnerumleitung mit beiden Richtlinienengines kann zu unvorhersehbarem Verhalten führen.

## Erweiterte Ordnerumleitung

In Bereitstellungen mit mehreren Betriebssystemen können Sie Teile eines Benutzerprofils für jedes Betriebssystem

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

freigeben. Der Rest des Profils ist nicht freigegeben und kann nur von einem Betriebssystem verwendet werden. Um sicherzustellen, dass die Benutzererfahrung für alle Betriebssysteme konsistent ist, benötigen Sie für jedes Betriebssystem eine andere Konfiguration. Dies ist die erweiterte Ordnerumleitung. Beispiel: Bei verschiedenen Versionen einer Anwendung auf zwei Betriebssystemen muss möglicherweise eine freigegebene Datei gelesen oder bearbeitet werden. Sie entscheiden daher, sie an einen einzigen Speicherort im Netzwerk umzuleiten, von dem beide Versionen auf sie zugreifen können. Oder Sie entscheiden, da die Inhalte des Startmenüordners der beiden Betriebssysteme unterschiedlich strukturiert sind, nur einen Ordner statt beide umzuleiten. Dadurch werden die Startmenüordner und die Inhalte auf jedem Betriebssystem getrennt, und die Benutzererfahrung ist konsistent.

Wenn Sie die erweiterte Ordnerumleitung in Ihrer Bereitstellung benötigen, müssen Sie die Struktur der Profildaten Ihrer Benutzer genau kennen und festlegen, welche Teile davon zwischen Betriebssystemen freigegeben werden können. Dies ist wichtig, weil eine falsch angewendete Ordnerumleitung zu unvorhersehbarem Verhalten führen kann.

Umleiten von Ordnern in erweiterten Bereitstellungen

- Verwenden Sie eine separate Bereitstellungsgruppe für jedes Betriebssystem.
- Informieren Sie sich, wo die Benutzerdaten und -einstellungen von den virtuellen Anwendungen, einschließlich solcher auf virtuellen Desktops, gespeichert werden, und wie die Daten strukturiert sind.
- Leiten Sie die Ordner bei freigegebenen Profildaten, bei denen ein sicheres Datenroaming gewährleistet ist (da sie in jedem Betriebssystem identisch strukturiert sind), in jeder Bereitstellungsgruppe um.
- Bei nicht freigegebenen Profildaten, für die kein Roaming möglich ist, leiten Sie den Ordner nur in einer Desktopgruppe um. Dies ist in der Regel diejenige mit dem am häufigsten verwendeten Betriebssystem oder diejenige mit den relevantesten Daten. Alternativ können Sie bei nicht freigegebenen Daten, für die kein Roaming zwischen Betriebssystemen möglich ist, die Ordner beider Betriebssysteme an separate Netzwerkadressen umleiten.

**Beispiel einer erweiterten Bereitstellung**: Diese Bereitstellung umfasst Anwendungen einschließlich Versionen von Microsoft Outlook und Internet Explorer, die auf Windows 8-Desktops und Anwendungen ausgeführt werden, sowie andere Versionen von Outlook und Internet Explorer, die von Windows Server 2008 bereitgestellt werden. Sie haben hierfür bereits zwei Bereitstellungsgruppen für die beiden Betriebssysteme eingerichtet. Die Benutzer möchten auf dieselben Kontakte und Favoriten in beiden Versionen dieser beiden Anwendungen zugreifen.
Wichtig: Die folgenden Entscheidungen und Hinweise gelten für die hier beschriebenen Betriebssysteme und die beschriebene Bereitstellung. Die Ordner, die Sie in Ihrer Organisation umleiten oder freigeben, hängen von mehreren Faktoren ab, die nur für Ihre Bereitstellung relevant sind.

- Sie leiten mit Richtlinien, die auf Bereitstellungsgruppen angewendet werden, die folgenden Ordner um:

| Ordner | Umleitung in Windows 8? | Umleitung in Windows Server 2008? |
|---|---|---|
| Dokumente | Ja | Ja |
| Anwendungsdaten | Nein | Nein |
| Kontakte | Ja | Ja |
| Desktop | Ja | Nein |
| Downloads | Nein | Nein |
| Favoriten | Ja | Ja |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Ordner | Umleitung in Windows 8? | Umleitung in Windows Server 2008? |
|---|---|---|
| Verknüpfungen | Ja | Nein |
| Musik | Ja | Ja |
| Bilder | Ja | Ja |
| Videos | Ja | Ja |
| Suchen | Ja | Nein |
| Gespeicherte Spiele | Nein | Nein |
| Startmenü | Ja | Nein |

- Bei freigegebenen, umgeleiteten Ordnern:
  - Nach der Analyse der Datenstruktur der von anderen Versionen von Outlook und Internet Explorer gespeicherten Daten entscheiden Sie, dass es sicher ist, die Ordner für Kontakte und Favoriten freizugeben.
  - Sie wissen, dass die Struktur der Ordner Eigene Dokumente, Musik, Bilder und Videos auf allen Betriebssystemen gleich ist, und sie können daher für jede Bereitstellungsgruppe am gleichen Netzwerkspeicherort gespeichert werden.
- Bei nicht freigegebenen, umgeleiteten Ordnern:
  - Die Ordner Desktop, Verknüpfungen, Suchen oder Startmenü werden nicht in die Windows Server-Bereitstellungsgruppe umgeleitet, da die Daten dieser Ordner unterschiedlich in den beiden Betriebssystemen organisiert sind. Eine Freigabe ist daher nicht möglich.
  - Um ein vorhersagbares Verhalten für diese nicht freigegebenen Daten sicherzustellen, leiten Sie sie nur in der Windows 8-Bereitstellungsgruppe um. Sie entscheiden dies, da Windows 8 öfter von den Benutzern bei ihrer täglichen Arbeit verwendet wird, die vom Server bereitgestellten Anwendungen hingegen werden nur gelegentlich genutzt. Außerdem sind in diesem Fall die nicht freigegebenen Daten relevanter für eine Desktop- als für eine Anwendungsumgebung. Desktopverknüpfungen werden beispielsweise im Ordner "Desktop" gespeichert und sind nützlich, wenn sie von einer Windows 8-Maschine, aber nicht von einem Windows-Server stammen.
- Bei nicht umgeleiteten Ordnern:
  - Die Server sollen keine von Benutzern heruntergeladene Dateien ansammeln, und Sie leiten den Ordner "Downloads" daher nicht um.
  - Daten von einzelnen Anwendungen können zu Kompatibilitäts- und Leistungsproblemen führen. Daher leiten Sie den Ordner "Anwendungsdaten" nicht um.

Weitere Informationen zur Ordnerumleitung finden Sie unter http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

### Ordnerumleitung und Ausschlüsse

In der Citrix Profilverwaltung (nicht aber in Studio) können Sie mit einer Leistungsverbesserung die Ordnerverarbeitung mit Ausschlüssen verhindern. Wenn Sie dieses Feature verwenden, schließen Sie keine umgeleiteten Ordner aus. Die Ordnerumleitung und die Ausschlussfunktion arbeiten zusammen, d. h. wenn Sie sicherstellen, dass keine umgeleiteten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ordner ausgeschlossen sind, können sie von der Profilverwaltung wieder in die Profilordnerstruktur verschoben werden, während gleichzeitig die Datenintegrität beibehalten wird, sollten sie später doch nicht umgeleitet werden. Weitere Informationen zu Ausschlüssen finden Sie unter Aufnehmen und Ausschließen von Objekten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Citrix Insight Services

Jul 08, 2016

Citrix Insight Services (CIS) ist die Flaggschiff-Plattform von Citrix für Diagnose und Problembehandlung. Mit ihr können hauseigene Experten des Kunden oder Partners Probleme diagnostizieren und beseitigen und die IT-Umgebung optimieren. Einzelheiten und aktuelle Informationen zu CIS und seiner Funktionsweise finden Sie unter https://cis.citrix.com (Citrix Anmeldeinformationen sind erforderlich).

Die zu Citrix Insight Services hochgeladenen Informationen werden für die Problembehandlung und zu Diagnosezwecken verwendet sowie zum Verbessern der Qualität, Zuverlässigkeit und Leistung von Produkten gemäß den folgenden Richtlinien:

- Citrix Insight Services-Richtlinie unter https://cis.citrix.com/legal
- Citrix Datenschutzrichtlinie unter http://www.citrix.com/about/legal/privacy.html

Dieses Release von XenApp und XenDesktop unterstützt die nachfolgend aufgeführten Tools und Technologien.

# Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Support fordert Sie u. U. auf, die Informationen hochzuladen, damit Citrix die Installationserfahrung von Kunden verbessern kann.

Die Informationen werden lokal unter %ProgramData%\Citrix\ gespeichert.

# Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit Citrix die Qualität und Leistung seiner Produkte verbessern kann. Weitere Informationen finden Sie unter http://more.citrix.com/XD-CEIP.

Beim Erstellen einer XenApp- oder XenDesktop-Site werden Sie automatisch für das Programm zur Verbesserung der Benutzerfreundlichkeit registriert. Der erste Datenupload erfolgt ca. sieben Tage nach dem Erstellen der Site. Sie können Ihre Teilnahme nach dem Erstellen der Site jederzeit beenden. Wählen Sie dazu im Navigationsbereich von Studio den Knoten **Konfiguration** (Registerkarte "Produktsupport") und folgen Sie den Anleitungen.

Sie können auch am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, wenn Sie andere Citrix Produkte, Komponenten und Technologien installieren, z. B. Provisioning Services, AppDNA, Citrix Lizenzserver, Citrix Receiver für Windows, den universellen Druckserver und Sitzungsaufzeichnung. Standardwerte für die Installation und Teilnahme finden Sie in der Dokumentation dieser Komponenten.

Bei dem Upgrade einer XenApp- oder XenDesktop-Bereitstellung:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP nicht unterstützte, werden Sie gefragt, ob Sie teilnehmen möchten.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme war aktiviert, ist CEIP in der aktualisierten Site aktiviert.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme war deaktiviert, ist CEIP in der aktualisierten Site deaktiviert.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme ist nicht bekannt, werden Sie gefragt, ob Sie teilnehmen möchten.

Die gesammelten Informationen sind anonym, daher können sie nach dem Upload auf Citrix Insight Services nicht angezeigt werden.

# Call Home

Wenn Sie bestimmte Komponenten und Features in XenApp oder XenDesktop installieren, wird Ihnen angeboten, an Citrix Call Home teilzunehmen. Call Home sammelt Diagnosedaten und lädt in regelmäßigen Abständen Telemetriepakete mit den Daten direkt nach Citrix Insight Services zur Analyse und Problembehandlung hoch.

Call Home wird als Hintergrunddienst unter dem Namen "Citrix Telemetry Service" ausgeführt.

Weitere Informationen finden Sie unter http://more.citrix.com/XD-CALLHOME.

**Folgendes wird gesammelt**

Die Citrix Diagnostic Facility (CDF)-Ablaufverfolgung protokolliert Informationen, die für die Problembehandlung hilfreich sein können. Call Home sammelt eine Untergruppe der CDF-Ablaufverfolgungen, die bei der Problembehandlung allgemeiner Fehler, z. B. bei VDA-Registrierungen und Starts von Anwendung und Desktops, hilfreich sein können. Diese Technologie wird auch als Always-On-Ablaufverfolgung (Always-On Tracing, AOT) bezeichnet. Call Home sammelt keine anderen ETW-Informationen (Ereignisablaufverfolgung für Windows) und kann auch nicht dafür konfiguriert werden.

Call Home sammelt auch andere Informationen, z. B.:

- Registrierungen, die von XenApp und XenDesktop in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix erstellt wurden
- Informationen zu Windows Management Instrumentation (WMI) unter dem Citrix Namespace
- Liste der aktuellen Prozesse
- Absturzabbilder von Citrix Prozessen, sie werden unter %PROGRAM DATA%\Citrix\CDF gespeichert

Die Ablaufverfolgungsinformationen werden bei der Sammlung komprimiert. Der Citrix Telemetriedienst speichert ca. 20 MB komprimierte Ablaufverfolgungsinformationen. Abhängig vom Umfang der Ablaufverfolgung während des Intervalls enthalten die Daten normalerweise Informationen zu den vergangenen 24 bis 48 Stunden.

- Durch das Komprimieren der Daten benötigt Call Home nicht viel Speicherplatz auf dem VDA.
- Ablaufverfolgungen bleiben im Speicher erhalten, damit auf bereitgestellten Maschinen keine IOPS erfolgen müssen.
- Der Ablaufverfolgungspuffer verwendet einen kreisförmigen Mechanismus, um Ablaufverfolgungen im Speicher zu erhalten.

## Konfigurations- und Verwaltungszusammenfassung

Wenn Sie einen Delivery Controller oder VDA installieren, können Sie über die grafische Oberfläche im


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Produktinstallationsprogramm angeben, ob Sie an Call Home teilnehmen möchten.

Nach der Installation der Komponenten können Sie mit PowerShell-Cmdlets Folgendes festlegen:

- Aktivieren von geplanten Call Home-Uploads oder Ändern des aktuellen Zeitplans. Dies umfasst das Aktivieren von geplanten Uploads in einem Masterimage, das in einem Maschinenkatalog verwendet wird. Dadurch muss Call Home nicht in jeder erstellten VM konfiguriert werden.
- Manuelles Sammeln von Daten und Hochladen nach CIS.
- Manuelles Sammeln von Daten, lokale Speicherung und späterer Upload nach CIS.

Vollständige PowerShell-Cmdlet-Syntax finden Sie in der Cmdlet-Hilfe.

Bei der Registrierung für geplante Call Home-Uploads und beim manuellen Hochladen von Diagnoseinformationen nach CIS müssen Sie Citrix Kontoanmeldeinformationen angeben. CIS ersetzt die Anmeldeinformationen durch ein *Uploadtoken* zum Identifizieren des Kunden und Hochladen der Daten. Die Anmeldeinformationen werden nicht gespeichert.

Wenn Upload ausgeführt wird, wird per E-Mail eine Benachrichtigung an die Adresse des Citrix Kontos gesendet.

## Aktivieren und Konfigurieren von geplanten Uploads

Mit dem Assistenten des Produktinstallationsprogramms oder später mit PowerShell-Cmdlets können Sie sich für geplante Uploads nach Call Home registrieren. Standardmäßig werden Daten gesammelt und jeden Sonntag gegen 03:00 Uhr morgens (Ortszeit) nach CIS hochgeladen. Die Uploadzeit wird innerhalb eines 2-Stunden-Fensters ab dem angegebenen Zeitpunkt zufällig festgelegt. Dies bedeutet, dass ein Upload nach dem Standardzeitplan zwischen 03:00 und 05:00 Uhr morgens erfolgt.

Wenn Sie Informationspakete mit Diagnoseinformationen nicht einem Plan gemäß regelmäßig hochladen möchten, können Sie mit PowerShell-Cmdlets Call Home-Daten manuell sammeln und hochladen.

**Aktivieren von geplanten Uploads während der Komponenteninstallation**

Wenn Sie mit der grafischen Benutzeroberfläche des XenApp- und XenDesktop-Produktinstallationsprogramms einen Controller oder VDA installieren, können Sie angeben, ob Sie geplante Uploads nach Call Home durchführen möchten. In der Standardeinstellung ist die Teilnahme ausgewählt.

- Wenn Sie teilnehmen möchten, melden Sie sich mit Ihren Citrix Kontoanmeldeinformationen an CIS an.
- Wenn Sie nicht teilnehmen möchten (oder wenn Sie teilnehmen möchten, aber die Citrix Anmeldeinformationen konnten nicht validiert werden), lehnen Sie die Teilnahme auf der Seite des Assistenten ab. Sie können sich später nach dem Setup der Site mit PowerShell-Cmdlets registrieren.

**Aktivieren von geplanten Uploads mit PowerShell-Cmdlets**

Geben Sie die folgenden Cmdlets ein, um geplante Uploads von Call Home-Paketen mit Diagnoseinformationen an CIS zu aktivieren. Wenn Sie keine zusätzlichen Cmdlets für einen benutzerdefinierten Zeitplan eingeben, wird der Standardzeitplan verwendet.

```
$cred = Get-Credentials
Enable-CitrixCallHome -Credential $cred
```

Um sicherzustellen, dass geplante Uploads aktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte wiedergegeben werden: IsEnabled=True und IsMasterImage=False.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Aktivieren von geplanten Uploads für Maschinen, die von einem Masterimage erstellt wurden**

Wenn Sie geplante Uploads in einem Masterimage konfigurieren, brauchen Sie nicht jede einzelne im Maschinenkatalog erstellte Maschine zu konfigurieren.

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

Um sicherzustellen, dass geplante Uploads aktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte zurückgegeben werden: IsEnabled=True und IsMasterImage=True.

**Erstellen eines benutzerdefinierten Zeitplans**

Sie können einen benutzerdefinierten täglichen oder wöchentlichen Zeitplan erstellen.

```
$timespan = New-TimeSpan –Hours -Minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek -UploadFrequency {Daily|Weekly}
```

**Abbrechen von geplanten Uploads**

Geben Sie das folgende Cmdlet ein, um geplante Uploads zu stornieren. (Sie können mit PowerShell-Cmdlets trotzdem Pakete mit Diagnosedaten hochladen.)

```
Disable-CitrixCallHome
```

Um sicherzustellen, dass geplante Uploads deaktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte zurückgegeben werden: IsEnabled=False und IsMasterImage=False.

**Beispiele**

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete jeden Abend um 23:20 Uhr erstellt und hochgeladen werden.  Beachten Sie, dass der Parameter für Stunden das 24-Stunden-Format verwendet. Wenn der Wert für den Parameter "UploadFrequency" auf "Daily" festgelegt ist, wird der Parameter "DayOfWeek" ignoriert, wenn er angegeben ist.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Um den Zeitplan zu überprüfen, geben Sie Get-CitrixCallHomeSchedule ein. Für das oben aufgeführte Beispiel sollte Folgendes zurückgegeben werden: StartTime=22:20:00, DayOfWeek=Sunday (ignoriert), Upload Frequency=Daily.

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete mittwochabends um 23:20 Uhr erstellt und hochgeladen werden.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

Um den Zeitplan zu überprüfen, geben Sie Get-CitrixCallHomeSchedule ein. Für das oben aufgeführte Beispiel sollte Folgendes zurückgegeben werden: StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

## Manuelles Sammeln und Hochladen von Diagnoseinformationen

Sie können über die CIS-Website ein Diagnoseinformationspaket nach CIS hochladen. Sie können auch PowerShell-Cmdlets zum Sammeln und Hochladen von Diagnoseinformationen nach CIS verwenden.

Hochladen eines Pakets über die CIS-Website

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

1. Melden Sie sich mit Ihren Citrix Kontoanmeldeinformationen an Citrix Insight Services an.
2. Wählen Sie **My Workspace**.
3. Wählen Sie **Healthcheck** und navigieren Sie zum Speicherort der Daten.

CIS unterstützt mehrere PowerShell-Cmdlets, die Datenuploads verwalten. In dieser Dokumentation werden die Cmdlets für zwei häufige Fälle behandelt:

- Verwenden Sie das Cmdlet Start-CitrixCallHomeUpload, um ein Diagnoseinformationspaket manuell zu sammeln und nach CIS hochzuladen. (Das Paket wird nicht lokal gespeichert.)
- Verwenden Sie das Cmdlet Start-CitrixCallHomeUpload, um Daten manuell zu sammeln und ein Diagnoseinformationspaket lokal zu speichern. Auf diese Weise können Sie eine Vorschau der Daten anzeigen. Zu einem späteren Zeitpunkt können Sie dann das Cmdlet Send-CitrixCallHomeBundle verwenden, um eine Kopie des Pakets manuell nach CIS hochzuladen. (Die ursprünglichen Daten bleiben lokal gespeichert.)

Die PowerShell-Hilfe enthält umfassende Syntax, einschließlich Beschreibungen von Cmdlets und Parametern, die nicht so häufig verwendet werden.

Wenn Sie ein Cmdlet zum Hochladen von Daten nach CIS eingeben, werden Sie aufgefordert, den Upload zu bestätigen. Wenn ein Timeout des Cmdlets erfolgt, bevor der Upload abgeschlossen ist, überprüfen Sie den Status des Uploads im Systemereignisprotokoll. Die Uploadanforderung wird möglicherweise abgelehnt, wenn der Dienst bereits einen Upload ausführt.

**Sammeln von Daten und Hochladen des Pakets nach CIS**

Start-CitrixCallHomeUpload [-Credential] [-InputPath ] [-Description ] [-IncidentTime ] [-SRNumber ] [-Name ] [-UploadHeader ] [-AppendHeaders ] [-Collect ] []

**Sammeln von Daten und lokales Speichern**

Start-CitrixCallHomeUpload -OutputPath [-InputPath ] [-Description ] [-IncidentTime ] [-SRNumber ] [-Name ] [-UploaderHeader ] [-AppendHeaders ] [-Collect ] []

| Parameter | Beschreibung |
|---|---|
| Credential | Leitet den Upload nach CIS. |
| InputPath | Speicherort der ZIP-Datei, die zum Paket gehört. Das kann eine weitere Datei sein, die Citrix Support benötigt. Stellen Sie sicher, dass die Erweiterung .zip eingeschlossen ist. |
| OutputPath | Speicherort, an dem die Diagnoseinformationen gespeichert werden. Dieser Parameter ist erforderlich, wenn Call Home-Daten lokal gespeichert werden. |
| Description and Incident Time | Formlose Informationen zum Upload. |
| SRNumber | Incident-Nummer des technischen Supports von Citrix. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Name | Name des Pakets. |
| UploadHeader | Zeichenfolge im JSON-Format zur Angabe der Uploadheader, die nach CIS hochgeladen werden. |
| AppendHeaders | Zeichenfolge im JSON-Format zur Angabe der angefügten Header, die nach CIS hochgeladen werden. |
| Collect | Zeichenfolge im JSON-Format zur Angabe, welche Daten gesammelt oder ausgelassen werden, das Format ist {'collector':{'enabled':Boolean}}", wobei Boolean "true" oder "false" ist.<br><br>Gültige Datensammelpunktwerte sind:<br><br>• 'wmi'<br>• 'process'<br>• 'registry<br>• "crashreport'<br>• 'trace'<br>• 'localdata'<br>• 'sitedata'<br><br>Wenn dieser Parameter nicht angegeben wird, werden Daten von allen Datensammelpunkten gesammelt. |
| Common Parameters | Weitere Informationen finden Sie in der PowerShell-Hilfe. |

**Hochladen von Daten, die zuvor lokal gespeichert waren**

```
Send-CitrixCallHomeBundle -Credential -Path []
```

Mit dem Path-Parameter geben Sie den Speicherort des zuvor gespeicherten Pakets an.

**Beispiele**

Mit dem folgenden Cmdlet wird ein Upload von Call Home-Daten (mit Ausnahme von Daten vom WMI-Datensammelpunkt) nach CIS angefordert. Diese Daten beziehen sich auf Registrierungsfehler bei PVS VDAs, die um 14:30 Uhr für den Citrix Supportfall 123456 bemerkt wurden. Zusätzlich zu den Call Home-Daten wird die Datei c:\Diagnostics\ExtraData.zip in das Uploadpaket eingeschlossen.

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

Das folgende Cmdlet speichert Call Home-Daten, die sich auf den Citrix Supportfall 223344 beziehen, der um 8:15 Uhr bemerkt wurde. Die Daten werden in der Datei mydata.zip auf einer Netzwerkfreigabe gespeichert. Zusätzlich zu den Call


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Home-Daten wird die Datei c:\Diagnostics\ExtraData.zip in das gespeicherte Paket eingeschlossen.

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath
"c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -
SRNumber 223344
```

Das folgende Cmdlet lädt das Datenpaket hoch, das Sie zuvor gespeichert haben.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überwachung

Jul 08, 2016

Administratoren und Helpdesk-Mitarbeiter können XenApp- und XenDesktop-Sites mit einer Reihe von Features und Tools überwachen. Sie können Folgendes überwachen:

- Benutzersitzungen und Sitzungsverwendung
- Anmeldungsleistung
- Verbindungen und Computer, einschließlich Ausfälle
- Lastauswertung
- Historische Trends
- Infrastruktur

**Citrix Director**

Director ist ein Echtzeit-Webtool, mit dem Sie Endbenutzer überwachen, Fehler beheben und Support leisten können.

Weitere Informationen finden Sie in den Artikeln zu Director.

**Sitzungsaufzeichnung**

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in der Sitzung eines Benutzers über eine beliebige Verbindung von einem XenApp-Server (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung verwendet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungssitzungen ausgelöst werden können. Das IT-Team kann damit die Benutzeraktivität von Anwendungen überwachen und prüfen, z. B. Buchhaltungs- und Patienteninformationssysteme für das Gesundheitswesen, und interne Kontrollen zur Einhaltung von gesetzlichen Vorschriften und die Sicherheitsüberwachung unterstützen. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

Weitere Informationen finden Sie in den Artikeln zur Sitzungsaufzeichnung.

**Konfigurationsprotokollierung**

Die Konfigurationsprotokollierung ist ein Feature, mit dem Administratoren administrative Änderungen verfolgen, die an einer Site vorgenommen werden. Die Konfigurationsprotokollierung ermöglicht Administratoren die Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen, Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen sowie Berichte über Administratoraktivitäten.

Sie können Berichte mit protokollierten Informationen über Studio generieren und anzeigen. Zum Zweck der Benachrichtigung über Konfigurationsänderungen können Sie protokollierte Elemente außerdem in der Trendansicht von Director anzeigen. Dieses Feature ist für Administratoren nützlich, die keinen Zugriff auf Studio haben.

Die Trendansicht bietet historische Daten von Konfigurationsänderungen in einem bestimmten Zeitraum, sodass Administratoren beurteilen können, welche Änderungen wann und von wem an einer Site vorgenommen wurden, um die Ursache eines Problems zu finden. Konfigurationsinformationen werden in dieser Ansicht in drei Kategorien unterteilt.

- Verbindungsfehler


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Fehlgeschlagene Desktopmaschinen
- Fehlgeschlagene Servermaschinen

Weitere Informationen zum Aktivieren und Konfigurieren der Konfigurationsprotokollierung finden Sie im Artikel Konfigurationsprotokollierung. Im Artikel Director wird beschrieben, wie protokollierte Informationen über dieses Tool angezeigt werden.

**Überwachungsdienst-API mit OData-Protokoll**

Mit der Überwachungsdienst-API einer Site können Administratoren unter Verwendung des OData-Protokolls historische Daten durchsuchen. Dies ermöglicht IT-Mitarbeitern das Analysieren historischer Trends für die Planung, das Durchführen gezielter Problembehandlung bei Verbindungs- und Maschinenfehlern und das Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse.

Das Schema des Überwachungsdiensts bietet folgende Datentypen:

- Daten zu Verbindungsfehlern
- Maschinen in fehlerhaftem Zustand
- Sitzungsnutzung
- Anmeldedauer
- Daten zum Lastausgleich

Weitere Informationen finden Sie in den Artikeln zur Überwachungsdienst-OData-API.

**Diagnose Tool für persönliche vDisks**

Mit dem PvD-Diagnosetool können Sie Änderungen überwachen, die Benutzer an Benutzer- und Anwendungskomponenten ihrer persönlichen vDisks vornehmen, z. B. Installation von Anwendungen oder Änderungen an Dateien.

Weitere Informationen finden Sie in dem Artikel Überwachen von Personal vDisks.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sitzungsaufzeichnung

Jul 08, 2016

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in der Sitzung eines Benutzers von einer VDI-Serverbetriebssystemmaschine über eine beliebige Verbindung (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung verwendet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungssitzungen ausgelöst werden können. Das IT-Team kann damit die Benutzeraktivität von Anwendungen, z. B. Buchhaltungs- und Patienteninformationssysteme für das Gesundheitswesen, überwachen und interne Kontrollen zur Einhaltung von gesetzlichen Vorschriften und die Sicherheitsüberwachung unterstützen. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

## Vorteile

**Erhöhte Sicherheit durch Protokollierung und Überwachung**: Mit der Sitzungsaufzeichnung können Unternehmen die Aktivität der Benutzer auf dem Bildschirm für Anwendungen aufzeichnen, die vertrauliche Informationen verarbeiten. Dies ist besonders in stark regulierten Branchen wichtig, z. B. im Gesundheits- und Finanzwesen. Richtliniensteuerelemente ermöglichen eine selektive Aufzeichnung, wenn persönliche Daten ins Spiel kommen, die nicht aufgezeichnet werden dürfen.

**Leistungsfähige Aktivitätsüberwachung**: Die Sitzungsaufzeichnung erfasst und archiviert Bildschirmaktualisierungen, einschließlich Mausklicks und die visuelle Ausgabe von Tastaturanschlägen in gesicherten Videoaufzeichnungen, um die Aktivität für bestimmte Benutzer, Anwendungen und Server zu dokumentieren.

Die Sitzungsaufzeichnung ist nicht dafür ausgelegt oder vorgesehen, Beweismittel für Rechtsverfahren zu sammeln. Citrix empfiehlt, dass Unternehmen, die die Sitzungsaufzeichnung verwenden, andere Methoden der Beweismittelsammlung nutzen, z. B. konventionelle Videoaufzeichnungen in Kombination mit textbasierten eDiscovery-Tools.

**Schnellere Problembehebung**: Wenn sich Benutzer mit einem Problem an den Helpdesk wenden, das schwer zu reproduzieren ist, können die Supportmitarbeiter die Aufzeichnung von Benutzersitzungen aktivieren. Wenn das Problem wieder auftritt, stellt die Sitzungsaufzeichnung eine visuelle Aufzeichnung des Fehlers bereit, einschließlich Zeitstempel, mit der Benutzerprobleme schneller gelöst werden können.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erste Schritte mit der Sitzungsaufzeichnung

Jul 08, 2016

Nach dem Durchführen der folgenden Schritte können Sie XenApp- und XenDesktop-Sitzungen aufzeichnen und prüfen.

1. Machen Sie sich mit den Komponenten der Sitzungsaufzeichnung vertraut.
2. Wählen Sie das Bereitstellungsszenario für die Umgebung.
3. Prüfen Sie die Installationsanforderungen.
4. Installieren Sie die erforderlichen Windows-Rollen und -Features.
5. Installieren Sie die Sitzungsaufzeichnung.
6. Konfigurieren Sie die Sitzungsaufzeichnungskomponenten für das Aufzeichnen und Anzeigen von Sitzungen.

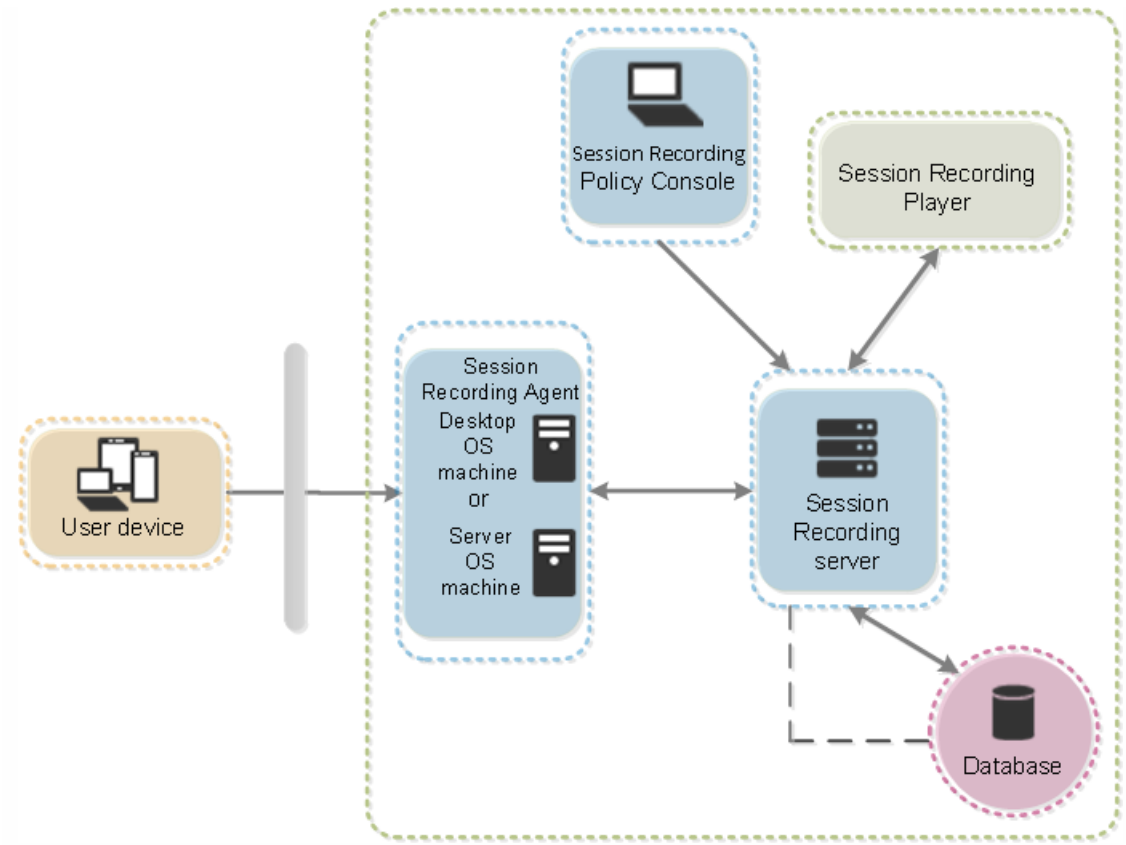
Die Sitzungsaufzeichnung besteht aus fünf Komponenten:

- **Sitzungsaufzeichnungsagent:** Komponente, die auf jeder Serverbetriebssystem- und VDI-Maschine zum Aktivieren der Aufzeichnungen installiert ist. Mit dieser Komponente werden Sitzungsdaten aufgezeichnet.
- **Sitzungsaufzeichnungsserver:** Ein Server, auf dem die folgenden Programme ausgeführt werden:
  - Broker: Eine von IIS 6.0+ gehostete Webanwendung, die Such- und Dateidownloadanfragen vom Player und Richtlinienverwaltungsanforderungen von der Sitzungsaufzeichnungs-Richtlinienkonsole handhabt und Aufzeichnungsrichtlinien für jede XenApp- und XenDesktop-Sitzung auswertet.
  - Speichermanager: Ein Windows-Dienst, der Sitzungsaufzeichnungsdateien verwaltet, die von jedem für die Sitzungsaufzeichnung aktivierten Computer mit XenApp bzw. XenDesktop empfangen werden.
- **Sitzungsaufzeichnungsplayer:** Eine Benutzeroberfläche, auf die Benutzer von der Arbeitsstation aus zugreifen und mit der aufgezeichnete XenApp- bzw. XenDesktop-Sitzungsdateien wiedergegeben werden.
- **Datenbank für die Sitzungsaufzeichnung:** eine Komponente, die die SQL Server-Datenbank zum Speichern von Sitzungsaufzeichnungsdaten verwaltet. Wenn diese Komponente installiert ist, erstellt sie eine Datenbank mit dem Namen **CitrixSessionRecording**. Der Name kann nicht geändert werden.
- **Richtlinienkonsole für die Sitzungsaufzeichnung**: Konsole zum Erstellen von Richtlinien, um anzugeben, welche Sitzungen aufgezeichnet werden sollen.

In dieser Abbildung werden die Komponenten der Sitzungsaufzeichnung und deren Beziehung zueinander dargestellt:

Im dargestellten Beispiel einer Bereitstellung befinden sich der Sitzungsaufzeichnungsagent, der Sitzungsaufzeichnungsserver, die Datenbank für die Sitzungsaufzeichnung, die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer hinter einer Sicherheitsfirewall. Der Sitzungsaufzeichnungsagent ist auf einer Serverbetriebssystemmaschine installiert. Auf einem zweiten Server wird die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt, ein dritter Server ist der Sitzungsaufzeichnungsserver und auf einem vierten Server wird die Datenbank für die Sitzungsaufzeichnung ausgeführt. Der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert. Ein Clientgerät außerhalb der Firewall kommuniziert mit der Serverbetriebssystemmaschine, auf der der Sitzungsaufzeichnungsagent installiert ist. Innerhalb der Firewall kommunizieren der Sitzungsaufzeichnungsagent, die Richtlinienkonsole für die Sitzungsaufzeichnung, der Sitzungsaufzeichnungsplayer und die Datenbank für die Sitzungsaufzeichnung mit dem Sitzungsaufzeichnungsserver.


© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Planen der Bereitstellung

Jul 08, 2016

### Einschränkungen und Hinweise

Die Sitzungsaufzeichnung unterstützt nicht den Anzeigemodus der Desktopgestaltungsumleitung (DCR). Wenn eine Sitzung gemäß Aufzeichnungsrichtlinie aufgezeichnet werden muss, deaktiviert die Sitzungsaufzeichnung standardmäßig DCR für diese Sitzung. Sie können dieses Verhalten in den Eigenschaften des Sitzungsaufzeichnungsagents konfigurieren.

Abhängig von der Umgebung können Sie die Sitzungsaufzeichnungskomponenten in verschiedenen Szenarios bereitstellen.

Eine Sitzungsaufzeichnungsbereitstellung muss nicht auf eine Site begrenzt sein. Außer dem Sitzungsaufzeichnungsagent sind alle Komponenten von der Serversite unabhängig. Sie können beispielsweise mehrere Sites für einen Sitzungsaufzeichnungsserver konfigurieren.

Wenn Sie jedoch eine große Site mit vielen Instanzen der Agentsoftware haben und viele grafikintensive Anwendungen (z. B. AutoCAD-Anwendungen) oder viele Sitzungen aufzeichnen möchten, kann dies zu einem hohen Leistungsbedarf auf einem Sitzungsaufzeichnungsserver führen. Sie können zur Vermeidung von Leistungsproblemen mehrere Sitzungsaufzeichnungsserver auf verschiedenen Computern installieren und die Instanzen des Sitzungsaufzeichnungsagents auf verschiedene Computer verweisen. Vergessen Sie jedoch nicht, dass eine Instanz der Agentsoftware nur jeweils auf einen Server verweisen kann.

### Empfohlene Bereitstellungsszenarios

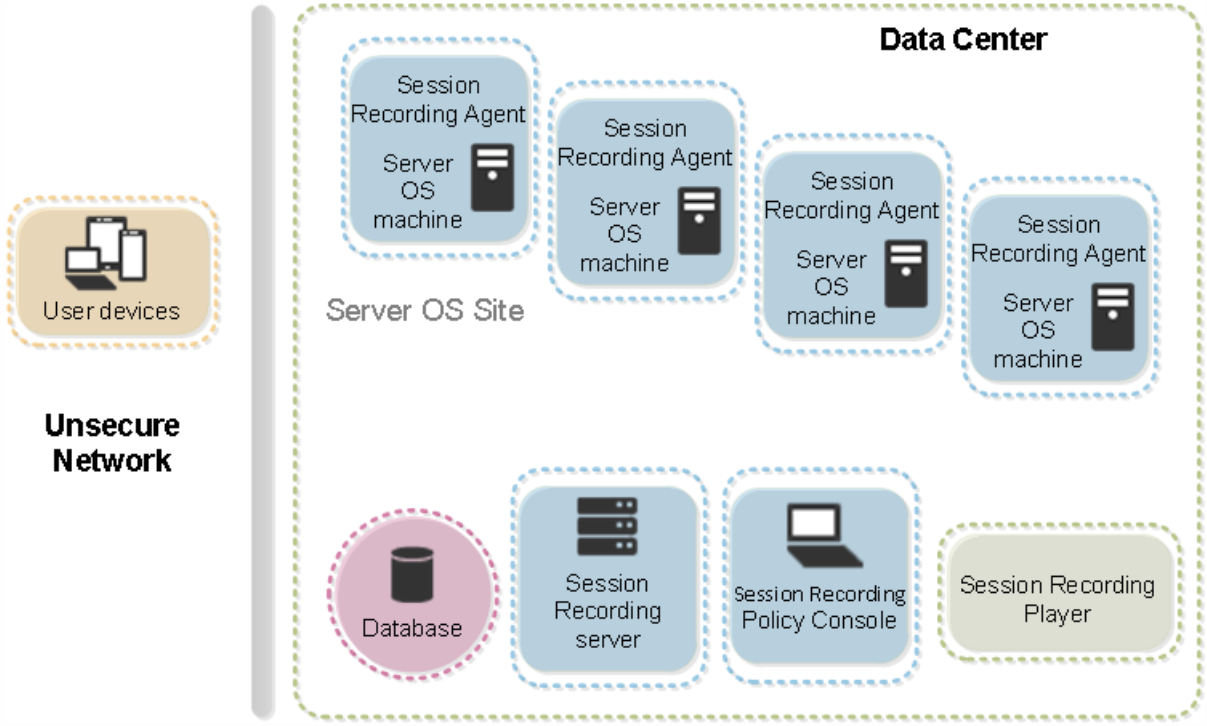
Im Anschluss finden Sie die zwei empfohlenen Konfigurationen für eine Sitzungsaufzeichnungsbereitstellung:

- Bereitstellen des Sitzungsaufzeichnungsagents auf einer einzelnen Serverbetriebssystemmaschine
- Bereitstellen des Sitzungsaufzeichnungsagents auf mehreren Server- oder Desktopbetriebssystemmaschinen

## Serversitebereitstellung

Verwenden Sie diesen Typ der Bereitstellung für die Aufzeichnung von Sitzungen für eine oder mehrere Sites. Der Sitzungsaufzeichnungsagent wird auf jeder Serverbetriebssystemmaschine der Site installiert. Die Site befindet sich in einem Datencenter hinter einer Sicherheitsfirewall. Die Komponenten der Sitzungsaufzeichnungsverwaltung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver, Richtlinienkonsole für die Sitzungsaufzeichnung) sind außerhalb des Datencenters hinter der Firewall auf anderen Servern und der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert. Außerhalb der Firewall, in einer nicht gesicherten Netzwerkumgebung, befinden sich die XenApp-Clients, z. B. Arbeitsstationen, mobile Geräte, PDAs und Laptops.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Wichtige Bereitstellungshinweise

- Die Komponenten der Sitzungsaufzeichnung können nur miteinander kommunizieren, wenn sie in derselben Domäne oder in vertrauenswürdigen Domänen mit einer gegenseitigen Vertrauensbeziehung installiert sind. Das System kann nicht in einer Arbeitsgruppe oder in Domänen mit einer externen Vertrauensbeziehung installiert werden.
- Die Sitzungsaufzeichnung unterstützt kein Clustering von zwei oder mehr Sitzungsaufzeichnungsservern in einer Bereitstellung.
- Aufgrund des hohen Grafikanteils und der Speichernutzung bei der Wiedergabe von großen Aufzeichnungen sollte der Sitzungsaufzeichnungsplayer nicht als veröffentlichte Anwendung installiert werden.
- Die Installation der Sitzungsaufzeichnung ist für die TLS/HTTPS-Kommunikation konfiguriert. Stellen Sie sicher, dass Sie ein Zertifikat auf dem Sitzungsaufzeichnungsserver installieren, und dass die Komponenten der Sitzungsaufzeichnung der Stammzertifizierungsstelle vertrauen.
- Wenn Sie die Datenbank für die Sitzungsaufzeichnung auf einem eigenständigen Server mit SQL Server 2014 Express Edition, SQL Server 2012 Express Edition oder SQL Server 2008 R2 Express Edition ausführen, muss auf dem Server das TCP/IP-Protokoll aktiviert sein und der SQL Server-Browserdienst muss ausgeführt werden. Diese Einstellungen sind standardmäßig deaktiviert, müssen jedoch für die Kommunikation zwischen dem Sitzungsaufzeichnungsserver und der Datenbank aktiviert werden. Weitere Informationen zur Aktivierung dieser Einstellungen finden Sie in der Microsoft Dokumentation.
- Berücksichtigen Sie bei der Planung der Sitzungsaufzeichnungsbereitstellung die Auswirkungen der Sitzungsfreigabe. Die Sitzungsfreigabe für veröffentlichte Anwendungen kann Konflikte mit Richtlinienregeln für Sitzungsaufzeichnungen der Sitzungsaufzeichnung für veröffentlichte Anwendungen verursachen. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Wenn der Benutzer die erste Anwendung geöffnet hat, halten weitere Anwendungen, die in derselben Sitzung geöffnet werden, die Richtlinie ein, die für die erste Anwendung gilt. Beispiel: Wenn eine Richtlinie festlegt, dass nur Outlook aufgezeichnet wird, beginnt die Aufzeichnung, wenn der Benutzer Outlook öffnet. Wenn der Benutzer jedoch Microsoft Word als zweite veröffentlichte Anwendung öffnet (während Outlook ausgeführt wird), wird Word auch aufgezeichnet. Sollte die aktive Richtlinie jedoch nicht festlegen, dass Word aufgezeichnet wird, und der Benutzer startet Word vor Outlook (gemäß der Richtlinie wird Outlook aufgezeichnet), wird Outlook nicht aufgezeichnet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Das Installieren des Sitzungsaufzeichnungsservers auf einem Delivery Controller kann zu Leistungsbeeinträchtigungen führen und empfiehlt sich daher nicht; es ist jedoch grundsätzlich möglich.
- Sie können die Richtlinienkonsole für die Sitzungsaufzeichnung auf einem Delivery Controller installieren.
- Sie können den Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung auf demselben System installieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sicherheitsempfehlungen

Jul 08, 2016

Die Sitzungsaufzeichnung ist für die Bereitstellung in einem sicheren Netzwerk und den Zugriff durch Administratoren konzipiert und ist daher sicher. Die Standardbereitstellung ist einfach, und Sicherheitsfunktionen, z. B. digitale Signatur und Verschlüsselung, können optional konfiguriert werden.

Die Komponenten der Sitzungsaufzeichnung kommunizieren über die Internetinformationsdienste (IIS) und Microsoft Message Queuing (MSMQ). Internetinformationsdienste stellen die Webdienste-Kommunikationsverbindung zwischen jeder Komponente der Sitzungsaufzeichnung bereit. MSMQ bietet eine zuverlässige Datentransportmethode zum Senden von Sitzungsaufzeichnungsdaten vom Sitzungsaufzeichnungsagent zum Sitzungsaufzeichnungsserver.

Berücksichtigen Sie diese Sicherheitsempfehlungen bei der Planung der Bereitstellung:

- Die verschiedenen Administratorrollen im Unternehmensnetzwerk, in der Sitzungsaufzeichnung und auf einzelnen Maschinen müssen ordnungsgemäß isoliert werden. Andernfalls besteht Gefahr durch Sicherheitsbedrohungen Gefahr für den Systembetrieb und das System kann zweckentfremdet verwendet werden. Citrix empfiehlt die Zuweisung verschiedener Administratorrollen an verschiedene Personen oder Konten, normale Sitzungsbenutzer sollten keine Administratorberechtigungen für das VDA-System erhalten.
  - Administratoren von XenApp und XenDesktop dürfen keinem Benutzer von veröffentlichten Anwendungen oder Desktops die lokale Administratorrolle für den VDA zuweisen. Wird die lokale Administratorrolle benötigt, schützen Sie die Komponenten des Sitzungsaufzeichnungsagents über Windows-Methoden oder die Lösung eines anderen Herstellers.
  - Weisen Sie die Administratorrollen für die Datenbank und die Richtlinie der Sitzungsaufzeichnung separat zu.
  - Citrix empfiehlt, dass Sie VDA-Administratorrechte nicht allgemeinen Sitzungsbenutzern zuweisen, besonders, wenn Remote-PC-Zugriff verwendet wird.
  - Das lokale Administratorkonto des Sitzungsaufzeichnungsservers muss streng geschützt werden.
  - Steuern Sie den Zugriff auf Maschinen, auf denen der Sitzungsaufzeichnungsplayer installiert ist. Hat ein Benutzer keine Playerrollenberechtigung, weisen Sie ihm für keinerlei Player-Maschinen eine lokale Administratorrolle zu. Deaktivieren Sie den anonymen Zugriff.
  - Citrix empfiehlt die Verwendung einer physischen Maschine als Speicherserver für die Sitzungsaufzeichnung.

- Die Sitzungsaufzeichnung zeichnet Grafikaktivitäten ohne Berücksichtigung des Datenschutzes auf. Unter bestimmten Umständen können sensible Daten (z. B. Benutzeranmeldeinformationen, persönliche Daten oder Bildschirme von Drittanbietern) unbeabsichtigt aufgezeichnet werden. Ergreifen Sie folgende Maßnahmen, um ein Risiko zu vermeiden:

  + Deaktivieren Sie das Kernspeicherabbild für VDA-Maschinen, es sei denn, es wird zur Problembehandlung benötigt.

    Zum Deaktivieren des Kernspeicherabbilds gehen Sie folgendermaßen vor:

    1. Klicken Sie mit der rechten Maustaste auf "Arbeitsplatz" und dann auf "Eigenschaften".
    2. Klicken Sie auf die Registerkarte "Erweitert" und dann unter "Starten und Wiederherstellen" auf "Einstellungen".
    3. Wählen Sie für "Debuginformationen speichern" die Option "Keine".

    Weitere Informationen finden Sie in dem Microsoft-Artikel https://support.microsoft.com/en-us/kb/307973.

  + Stellen Sie sicher, dass keine in veröffentlichten lokalen und Webanwendungen oder unternehmensintern


© 1999-2017 Citrix Systems, Inc. All rights reserved.

verwendeten Anmelde- und Sicherheitsinformationen angezeigt werden, ansonsten werden diese durch die Sitzungsaufzeichnung aufgezeichnet.

+ Die Benutzer müssen vor Beginn einer ICA-Sitzung jede Anwendung schließen, in der u. U. vertrauliche Informationen angezeigt werden.

+ Sitzungseigentümer müssen die Teilnehmer darauf aufmerksam machen, dass Software von Online-Meetings und Remoteunterstützung im Rahmen einer Desktopsitzungsaufzeichnung aufgezeichnet werden kann.

+ Lassen für veröffentlichte Desktops und Anwendungen nur automatische Authentifizierungsmethoden (z. B. per Single Sign-On oder Smartcard) zu.

- Zur ordnungsgemäßen Funktion und zur Erfüllung von Sicherheitsanforderungen bei der Sitzungsaufzeichnung ist eine spezifische Hardware/-infrastruktur (z. B. Unternehmensnetzwerkgeräte, Betriebssystem) erforderlich. Sorgen Sie auf Infrastrukturebene dafür, dass diese Elemente weder beschädigt noch missbraucht werden können und dass die Sitzungsaufzeichnung sicher und zuverlässig ausgeführt wird.
  - Schützen und Sie die für die Sitzungsaufzeichnung verwendete Netzwerkinfrastruktur und sorgen Sie für deren zuverlässige Verfügbarkeit.
  - Citrix empfiehlt die Verwendung der Sicherheitslösung eines Drittanbieters oder von Windows-Mechanismen zum Schutz der Sitzungsaufzeichnungskomponenten. Die Sitzungsaufzeichnung umfasst folgende Komponenten:
    - Auf dem Sitzungsaufzeichnungsserver
      - Prozesse: SsRecStoragemanager.exe und SsRecAnalyticsService.exe
      - Dienste: CitrixSsRecStorageManager und CitrixSsRecAnalyticsService
      - Alle Dateien im Installationsordner des Sitzungsaufzeichnungsservers
      - Registrierungsschlüssel in HKLM\Software\Citrix\SmartAuditor\Server
    - Auf dem Sitzungsaufzeichnungsagent
      - Prozess: SsRecAgent.exe
      - Dienst: CitrixSmAudAgent
      - Alle Dateien im Installationsordner des Sitzungsaufzeichnungsagents
      - Registrierungsschlüssel in HKLM\Software\Citrix\SmartAuditor\Agent
- Schränken Sie über die Zugriffssteuerungsliste (ACL) für Message Queuing (MSMQ) auf dem Sitzungsaufzeichnungsserver VDA- und VDI-Maschinen ein, die MSMQ-Daten an den Sitzungsaufzeichnungsserver senden können, und blockieren Sie das Senden von Daten an den Sitzungsaufzeichnungsserver durch unbefugte Maschinen.

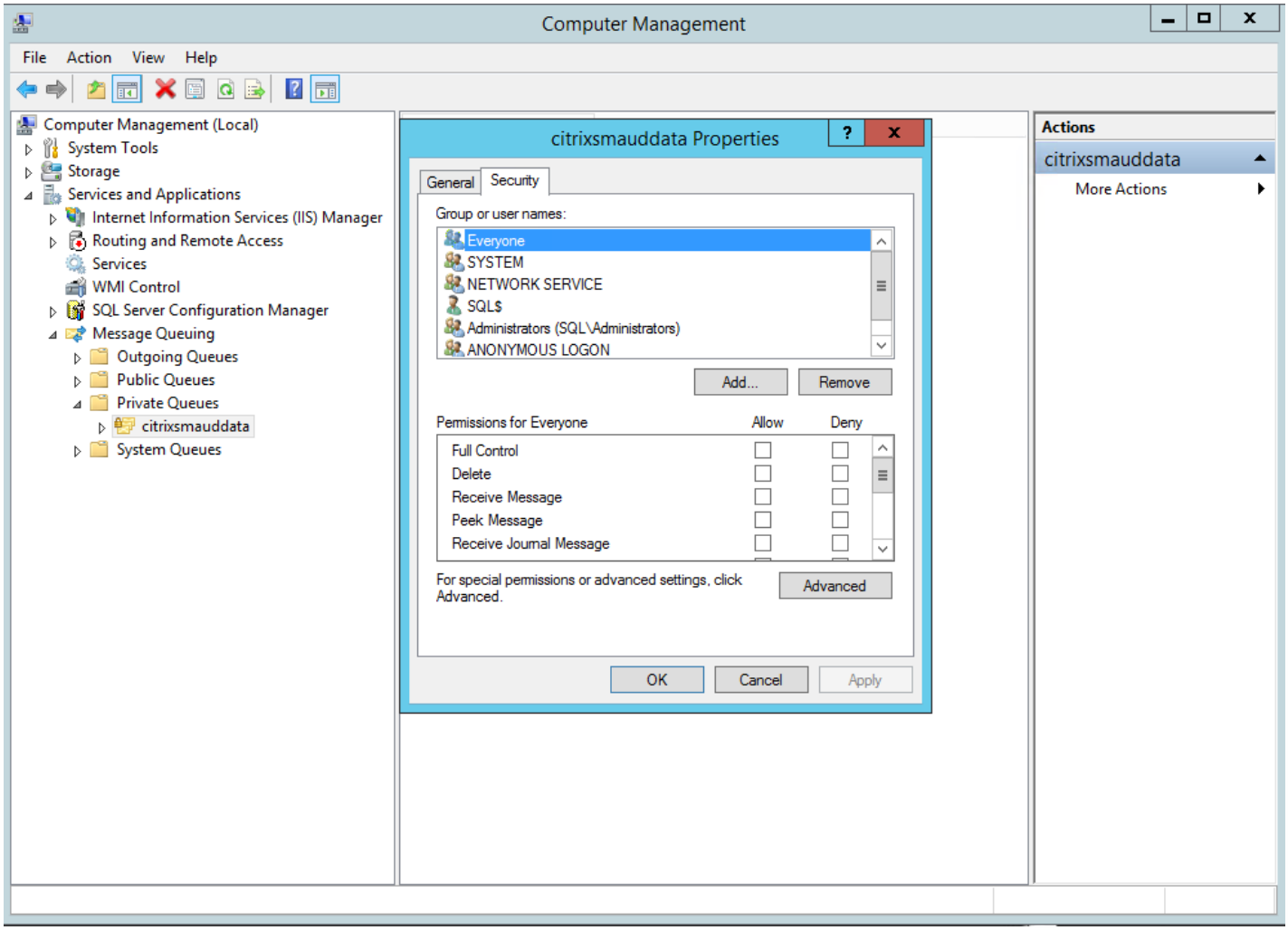
  1) Installieren Sie das Serverfeature Directory Service Integration auf jeder Sitzungsaufzeichnungsserver- und VDA- oder VDI-Maschine, auf der die Sitzungsaufzeichnung aktiviert ist, und starten Sie den Message Queuing-Dienst neu.

  2) Öffnen Sie auf jedem Sitzungsaufzeichnungsserver über das Windows-Startmenü **Verwaltungstools > Computerverwaltung**.

  3) Öffnen Sie **Dienste und Anwendungen > Message Queuing > Private Warteschlangen**.

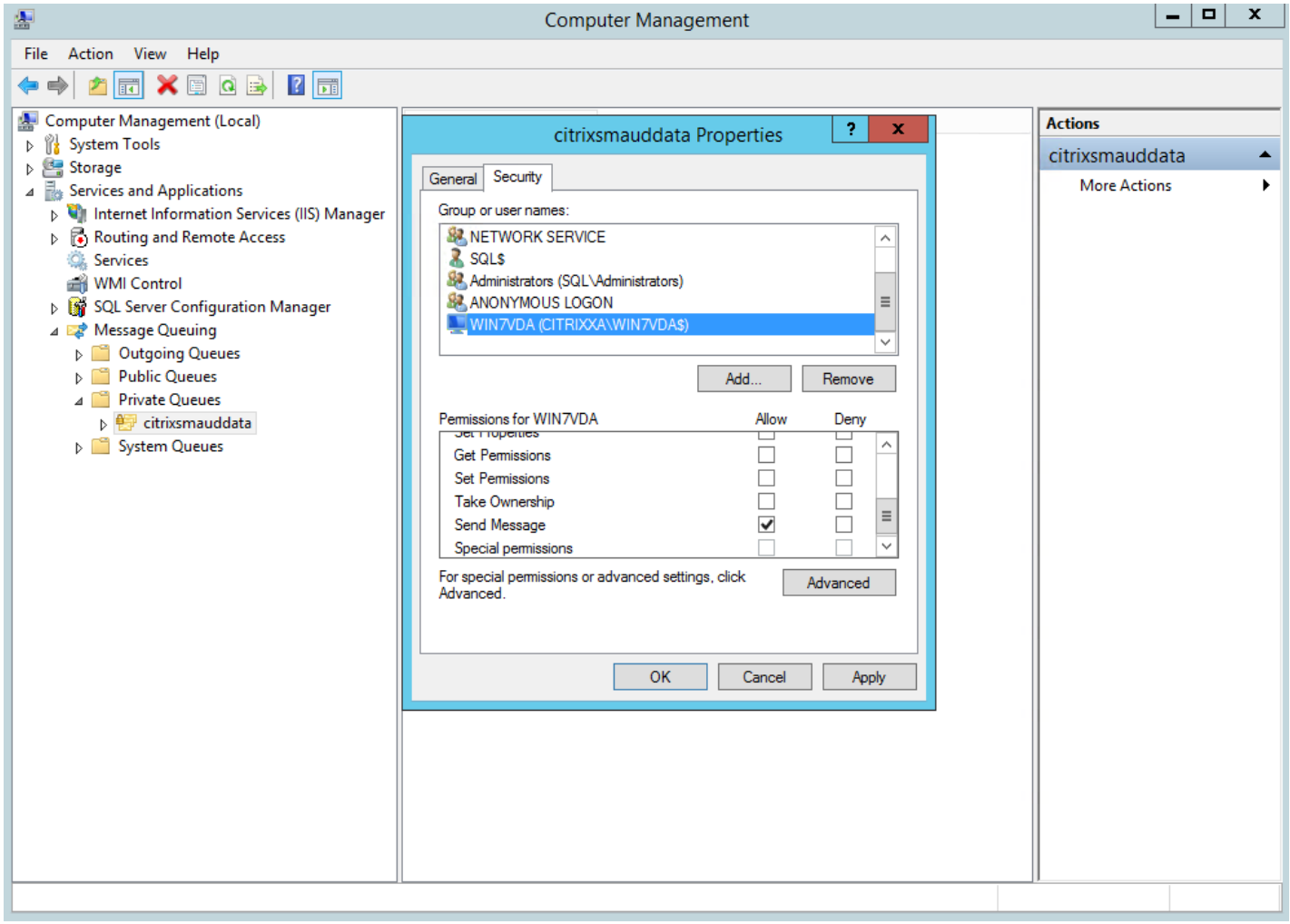
  4) Klicken Sie auf die private Warteschlange **citrixsmauddata**, um die Seite **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Sicherheit**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




5) Fügen Sie die Computer bzw. Sicherheitsgruppen der VDA-Maschinen, die MSMQ-Daten an diesen Server senden, hinzu und erteilen Sie diesen die Berechtigung zum Senden von Nachrichten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




- Schützen Sie das Ereignisprotokoll des Sitzungsaufzeichnungsservers und des Sitzungsaufzeichnungsagents. Citrix empfiehlt die Verwendung einer Remoteprotokollierungslösung eines Drittanbieters oder eines entsprechenden Windows-Features zum Schutz des Ereignisprotokolls oder dessen Umleitung auf einen Remoteserver.
- Stellen Sie sicher, dass Server mit Sitzungsaufzeichnungskomponenten physisch gesichert sind. Schließen Sie diese Computer falls möglich in einem sicheren Raum ein, zu dem nur autorisierte Person direkten Zugang haben.
- Isolieren Sie Server mit Sitzungsaufzeichnungskomponenten in einem separaten Subnetz oder einer separaten Domäne.
- Installieren Sie eine Firewall zwischen dem Sitzungsaufzeichnungsserver und den anderen Servern, um die aufgezeichneten Sitzungsdaten vor Benutzern zu schützen, die auf andere Server zugreifen.
- Halten Sie den Verwaltungsserver und die SQL-Datenbank für die Sitzungsaufzeichnung durch Installation der aktuellen Sicherheitsupdates von Microsoft auf dem neuesten Stand.
- Verhindern Sie, dass Personen ohne Administratorberechtigung sich beim Verwaltungscomputer anmelden.
- Schränken Sie genau ein, welche Benutzer die Aufzeichnungsrichtlinien ändern und Sitzungsaufzeichnungen anzeigen können.
- Installieren Sie digitale Zertifikate, verwenden Sie die Funktion zur Dateisignatur der Sitzungsaufzeichnung und richten Sie die TLS-Kommunikation in IIS ein.
- Legen Sie im Dialogfeld Sitzungsaufzeichnungsagent - Eigenschaften für MSMQ die Verwendung von HTTPS als Transportprotokoll fest. Weitere Informationen finden Sie unter Problembehandlung bei MSMQ.
- Verwenden Sie TSL 1.0 und deaktivieren Sie die Verschlüsselungsverfahren SSLv2, SSLv3 und RC4 auf dem Sitzungsaufzeichnungsserver und in der Datenbank für die Sitzungsaufzeichnung. Weitere Informationen finden Sie in


© 1999-2017 Citrix Systems, Inc. All rights reserved.

der Microsoft-Artikeln http://support.microsoft.com/default.aspx?scid=kb;en-us;187498 und http://support.microsoft.com/kb/245030/en-us.

- Verwenden Sie den Wiedergabeschutz. Der Wiedergabeschutz ist eine Funktion der Sitzungsaufzeichnung, mit der aufgezeichnete Dateien vor dem Download zum Sitzungsaufzeichnungsplayer verschlüsselt werden. Diese Option ist in der Standardeinstellung aktiviert und befindet sich in den Eigenschaften des Sitzungsaufzeichnungsservers.
- Stellen Sie die Sitzungsaufzeichnung nicht in einer öffentlichen Cloud, z. B. Amazon Web Services (AWS), bereit.
- Folgen Sie den Anleitungen von NSIT für die Länge der Kryptografieschlüssel und den Kryptografiealgorithmen.

Weitere Informationen über die Konfiguration der Sitzungsaufzeichnungsfeatures finden Sie unter http://support.citrix.com/article/CTX200868.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überlegungen zur Skalierbarkeit

Jul 08, 2016

Für die Installation und Ausführung der Sitzungsaufzeichnung sind im Vergleich zur Ausführung von XenApp nur wenige zusätzliche Ressourcen erforderlich. Wenn Sie jedoch viele Sitzungen mit der Sitzungsaufzeichnung aufzeichnen möchten oder die Sitzungen, die Sie aufzeichnen möchten, große Sitzungsdateien erstellen (z. B. Anwendungen mit hohem Grafikanteil), sollten Sie die Leistung des Systems berücksichtigen, wenn Sie die Bereitstellung der Sitzungsaufzeichnung planen.

Weitere Informationen finden zum Konstruieren eines flexibel skalierbaren Sitzungsaufzeichnungssystems finden Sie unter http://support.citrix.com/article/CTX200869.

Dieser Abschnitt enthält folgende Themen:

Empfehlungen zur Hardware

Datenträger- und Datenspeicherhardware

Netzwerkkapazität

Verarbeitungskapazität des Computers

Bereitstellen mehrerer Sitzungsaufzeichnungsserver

Datenbankskalierbarkeit

## Empfehlungen zur Hardware

Berücksichtigen Sie, wie viele Daten an jeden Sitzungsaufzeichnungsserver gesendet werden und wie schnell die Server diese Daten verarbeiten und speichern können. Die Rate, mit der das System die eingehenden Daten speichern kann, muss größer als die Dateneingaberate sein.

Sie können die Dateneingaberate schätzen, wenn Sie die Anzahl der aufgezeichneten Sitzungen mit der durchschnittlichen Größe jeder Sitzungsaufzeichnung multiplizieren und durch die Länge der Sitzungsaufzeichnungen dividieren. Beispiel: An einem 8-stündigen Arbeitstag zeichnen Sie 5000 Microsoft Outlook-Sitzungen auf, deren Größe 20 MB ist. Die Dateneingaberate beträgt dann ungefähr 3,5 MBit/s. (5000 Sitzungen multipliziert mit 20 MB, dividiert durch 8 Stunden und dividiert durch 3600 Sekunden.)

Sie können die Leistung steigern, wenn Sie die Leistung eines Sitzungsaufzeichnungsservers optimieren oder mehrere Sitzungsaufzeichnungsserver auf verschiedenen Computern installieren.

## Datenträger- und Datenspeicherhardware

Die Datenträger- und Datenspeicherhardware ist der wichtigste Faktor bei der Planung der Bereitstellung der Sitzungsaufzeichnung. Die Schreibleistung der Datenspeicherlösung ist besonders wichtig. Je schneller Daten zum Datenträger geschrieben werden, je höher ist die Leistung des Gesamtsystems.

Zu den für die Sitzungsaufzeichnung geeigneten Datenspeicherlösungen gehören lokale Datenträger, die als RAID-Arrays von einem lokalen Datenträgercontroller oder von einem verbundenen SAN gesteuert werden.

Hinweis: Die Sitzungsaufzeichnung sollte nicht mit NAS (Network-Attached Storage) verwendet werden, da Leistungs- und

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Sicherheitsprobleme auftreten, die mit dem Schreiben von Aufzeichnungsdaten in Netzlaufwerke verbunden sind.
Bei der Installation auf einem lokalen Datenträger steigert ein Datenträgercontroller mit integriertem Cachespeicher die Leistung. Ein Datenträgercontroller mit Cachespeicher muss eine Notstromversorgung durch Batterie haben, um die Datenintegrität bei einem Stromausfall sicherzustellen.

### Netzwerkkapazität

Ein Netzwerk mit 100 MBit/s ist für die Verbindung eines Sitzungsaufzeichnungsservers geeignet. Eine Gigabit-Ethernet-Verbindung kann die Leistung verbessern, führt jedoch nicht zu einer zehn Mal besseren Leistung als eine Verbindung mit 100 MBit/s.

Stellen Sie sicher, dass Netzwerkswitches, die von der Sitzungsaufzeichnung verwendet werden, nicht mit Anwendungen von Drittherstellern gemeinsam verwendet werden, die ggf. um die verfügbare Netzwerkbandbreite konkurrieren. Netzwerkswitches sollten nur vom Sitzungsaufzeichnungsserver verwendet werden.

### Verarbeitungskapazität des Computers

Der Computer, auf dem ein Sitzungsaufzeichnungsserver installiert ist, muss die folgenden Spezifikationen erfüllen:

- Eine Dual-CPU oder Dual-Core-CPU (empfohlen)
- 2 GB bis 4 GB RAM

Bei höheren Spezifikationen wird die Leistung nicht wesentlich gesteigert.

### Bereitstellen mehrerer Sitzungsaufzeichnungsserver

Wenn ein einzelner Sitzungsaufzeichnungsserver die Leistungsanforderungen nicht erfüllt, können Sie weitere Sitzungsaufzeichnungsserver auf anderen Computern installieren. Bei diesem Typ der Bereitstellung hat jeder Sitzungsaufzeichnungsserver eine dedizierte Datenspeicherung, Datenbank und dedizierte Netzwerkswitches. Verweisen Sie die Instanzen des Sitzungsaufzeichnungsagents in der Bereitstellung auf verschiedene Sitzungsaufzeichnungsserver, um die Last aufzuteilen.

### Datenbankskalierbarkeit

Die Datenbank für die Sitzungsaufzeichnung erfordert Microsoft SQL Server 2014, Microsoft SQL Server 2012 oder Microsoft SQL Server 2008 R2. Die an die Datenbank gesendete Datenmenge ist sehr gering, da nur die Metadaten über die aufgezeichneten Sitzungen in der Datenbank gespeichert werden. Die Sitzungsaufzeichnungsdateien werden auf einem separaten Datenträger gespeichert. Normalerweise benötigt jede aufgezeichnete Sitzung nur 1 KB in der Datenbank, es sei denn, Sie fügen durchsuchbare Ereignisse mit der Sitzungsaufzeichnungs-Ereignis-API in die Sitzung ein.

Bei den Express-Editionen von Microsoft SQL Server 2014, Microsoft SQL Server 2012, und Microsoft SQL Server 2008 R2 ist die Größe der Datenbank auf 10 GB beschränkt. Bei 1 KB pro aufgezeichneter Sitzung kann die Datenbank ungefähr 4 Millionen Sitzungen katalogisieren. Andere Editionen von Microsoft SQL Server haben keine Beschränkungen hinsichtlich Datenbankgröße und werden nur durch den verfügbaren Speicherplatz auf dem Datenträger beschränkt. Wenn die Zahl der Sitzungen in der Datenbank ansteigt, wird die Leistung der Datenbank und die Geschwindigkeit der Suchen nur geringfügig beeinträchtigt.

Wenn Sie keine Anpassungen über die Sitzungsaufzeichnungs-Ereignis-API machen, generiert jede aufgezeichnete Sitzung vier Datenbanktransaktionen: Zwei beim Start der Aufzeichnung, eine bei der Benutzeranmeldung bei der aufgezeichneten Sitzung und eine am Ende der Aufzeichnung. Beim Anpassen der Sitzungen mit der Sitzungsaufzeichnungs-Ereignis-API erstellt jedes durchsuchbare Ereignis, das aufgezeichnet wurde, eine Transaktion. Da selbst bei der einfachsten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Datenbankbereitstellung mehrere Hundert Transaktionen pro Sekunde gehandhabt werden können, wird die Verarbeitungslast für die Datenbank nie überstrapaziert. Die Auswirkung ist so gering, dass die Datenbank für die Sitzungsaufzeichnung normalerweise auf demselben SQL-Server wie andere Datenbanken ausgeführt werden kann, u. a. der XenApp- oder XenDesktop-Datenbank des Datenspeichers.

Wenn Sie in der Bereitstellung der Sitzungsaufzeichnung viele Millionen aufgezeichneter Sitzungen in der Datenbank katalogisieren müssen, halten Sie die Microsoft-Richtlinien zur Skalierbarkeit von SQL Server ein.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Installieren der Sitzungsaufzeichnung

Jul 08, 2016

Dieser Artikel enthält die folgenden Abschnitte:


Installationscheckliste

Hinzufügen erforderlicher Windows-Rollen und Features mit einem Skript

Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung

Installieren der Datenbank für die Sitzungsaufzeichnung

Installieren des Sitzungsaufzeichnungsservers

Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers

Installieren des Sitzungsaufzeichnungsagents

Installieren des Sitzungsaufzeichnungsplayers

Automatisieren der Installationen

Upgrade der Sitzungsaufzeichnung

Deinstallieren der Sitzungsaufzeichnung


## Installationscheckliste

Stellen Sie vor der Installation sicher, dass Sie die in dieser Liste aufgeführten Schritte abgeschlossen haben:

| ✓ | **Schritt** |
|---|---|
| | Installieren Sie die Voraussetzungen, bevor Sie mit der Installation beginnen. Informationen hierzu finden Sie unter Systemanforderungen und Hinzufügen erforderlicher Windows-Rollen und Features mit einem Skript. |
| | Wählen Sie die Computer aus, auf denen Sie die Komponenten der Sitzungsaufzeichnung installieren möchten, und stellen Sie sicher, dass jeder Computer die Hardware- und Softwareanforderungen für die zu installierenden Komponenten erfüllt. |
| | Laden Sie die Sitzungsaufzeichnung von der Citrix Downloadseite unter<br><br>XenApp > https://www.citrix.com/downloads/xenapp.html<br><br>oder<br><br>XenDesktop > https://www.citrix.com/downloads/xendesktop.html |
| | Installieren Sie die relevanten Zertifikate in der Umgebung, wenn die Kommunikation zwischen den Komponenten der Sitzungsaufzeichnung mit dem SSL-Protokoll erfolgt. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | Installieren Sie die für die Komponenten der Sitzungsaufzeichnung benötigten Hotfixes. Die Hotfixes sind unter Citrix Support verfügbar. |
| | Konfigurieren Sie Director zum Erstellen und Aktivieren von Sitzungsaufzeichnungsrichtlinien. Weitere Informationen finden Sie unter Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers. |

Hinweise:

- Citrix empfiehlt, die veröffentlichten Anwendungen in separate Bereitstellungsgruppen basierend auf den Aufzeichnungsrichtlinien aufzuteilen, da die Sitzungsfreigabe veröffentlichter Anwendungen einen Konflikt mit aktiven Richtlinien verursachen kann, wenn sie in derselben Bereitstellungsgruppe sind. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet.
- Wenn Sie beabsichtigen, Maschinenerstellungsdienste (MCS) oder Provisioning Services mit XenApp zu verwenden, bereiten Sie den Server für eine eindeutige QMID vor (s. Beschreibung unter "Bekannte Probleme"). Wenn Sie diesen Schritt nicht ausführen, verlieren Sie u. U. Aufzeichnungsdaten.
- Für SQL Server muss TCP/IP aktiviert sein, der SQL Server-Browserdienst muss ausgeführt und die Windows-Authentifizierung muss verwendet werden.
- Wenn Sie HTTPS verwenden, konfigurieren Sie Serverzertifikate für TLS/HTTPS.

Installationsdateien für die Sitzungsaufzeichnung:

- **Verwaltungsdateien der Sitzungsaufzeichnung**
  - Broker_PowerShellSnapIn_x64.msi
  - SessionRecordingAdministrationx64.msi
- **Agentdateien der Sitzungsaufzeichnung**
  - SessionRecordingAgentx64.msi
- **Playerdateien der Sitzungsaufzeichnung**
  - SessionRecordingPlayer.msi

### Hinzufügen erforderlicher Windows-Rollen und Features mit einem Skript

Damit die Sitzungsaufzeichnung ordnungsgemäß funktioniert, müssen Sie einige Windows-Rollen und -Features vor der Installation der Komponenten der Sitzungsaufzeichnung hinzufügen. Da die Suche und Installation einiger Rollen und Features u. U. schwierig ist, wird in diesem Abschnitt die Verwendung eines entsprechenden Skripts von Citrix erläutert. Führen Sie das Skript zum Installieren der Windows-Rollen und -Features aus, bevor Sie die Komponenten der Sitzungsaufzeichnung installieren.

## Installieren der erforderlichen Windows-Rollen und -Features

1. Wenn Sie die Citrix Skripts verwenden möchten konsultieren Sie den Artikel Skripts zum Hinzufügen erforderlicher Windows-Rollen und -Features.

2. Führen Sie auf der Maschine, auf der die Sie die Verwaltungskomponenten der Sitzungsaufzeichnung installieren möchten, die folgenden Schritte aus:

   a) Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

**Set-ExecutionPolicy RemoteSigned**

b) Starten Sie eine Eingabeaufforderung als Administrator und führen Sie folgenden Befehl aus:

**powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1**

Das Skript zeigt die erfolgreich hinzugefügten Features an und wird dann angehalten.

c) Stellen Sie nach der Skriptausführung sicher, dass die Ausführungsrichtlinie auf den für die Unternehmensrichtlinie erforderlichen Wert festgelegt ist.

3. Führen Sie auf der Maschine, auf der die Sie den Sitzungsaufzeichnungsagent installieren möchten, die folgenden Schritte aus:

a) Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.

**Set-ExecutionPolicy RemoteSigned**

b) Starten Sie eine Eingabeaufforderung als Administrator und führen Sie folgenden Befehl aus:

**powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1**

Das Skript zeigt die erfolgreich hinzugefügten Features an und wird dann angehalten.

c) Stellen Sie nach der Skriptausführung sicher, dass die Ausführungsrichtlinie auf den für die Unternehmensrichtlinie erforderlichen Wert festgelegt ist.

4. Nach Installation der Windows-Rollen und -Features installieren Sie die Sitzungsaufzeichnung.

## Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung

Die Verwaltungskomponenten der Sitzungsaufzeichnung sind die Datenbank für die Sitzungsaufzeichnung, der Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung. Sie können festlegen, welche dieser Komponenten auf einem Server installiert werden.

Stellen Sie sicher, dass alle Voraussetzungen installiert sind, bevor Sie die Verwaltungskomponenten der Sitzungsaufzeichnung installieren. Weitere Informationen finden Sie unter Systemanforderungen für die Sitzungsaufzeichnung.

Zum Verbessern der Sicherheit können Sie diese Berechtigungen nach der Installation der Datenbank entfernen.

1. Führen Sie **Broker_PowerShellSnapIn_x64.msi** aus und folgen Sie den Anweisungen zum Durchführen der Installation.
2. Rufen Sie eine Windows-Eingabeaufforderung als Administrator auf und führen Sie den Befehl **msiexec /i SessionRecordingAdministrationx64.msi** aus oder doppelklicken Sie auf die MSI-Datei.
3. Klicken Sie im Installationsprogramm auf **Weiter** und akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie im Setupbildschirm der Sitzungsaufzeichnungsverwaltung die Verwaltungskomponenten aus, die Sie installieren möchten.

## Installieren der Datenbank für die Sitzungsaufzeichnung

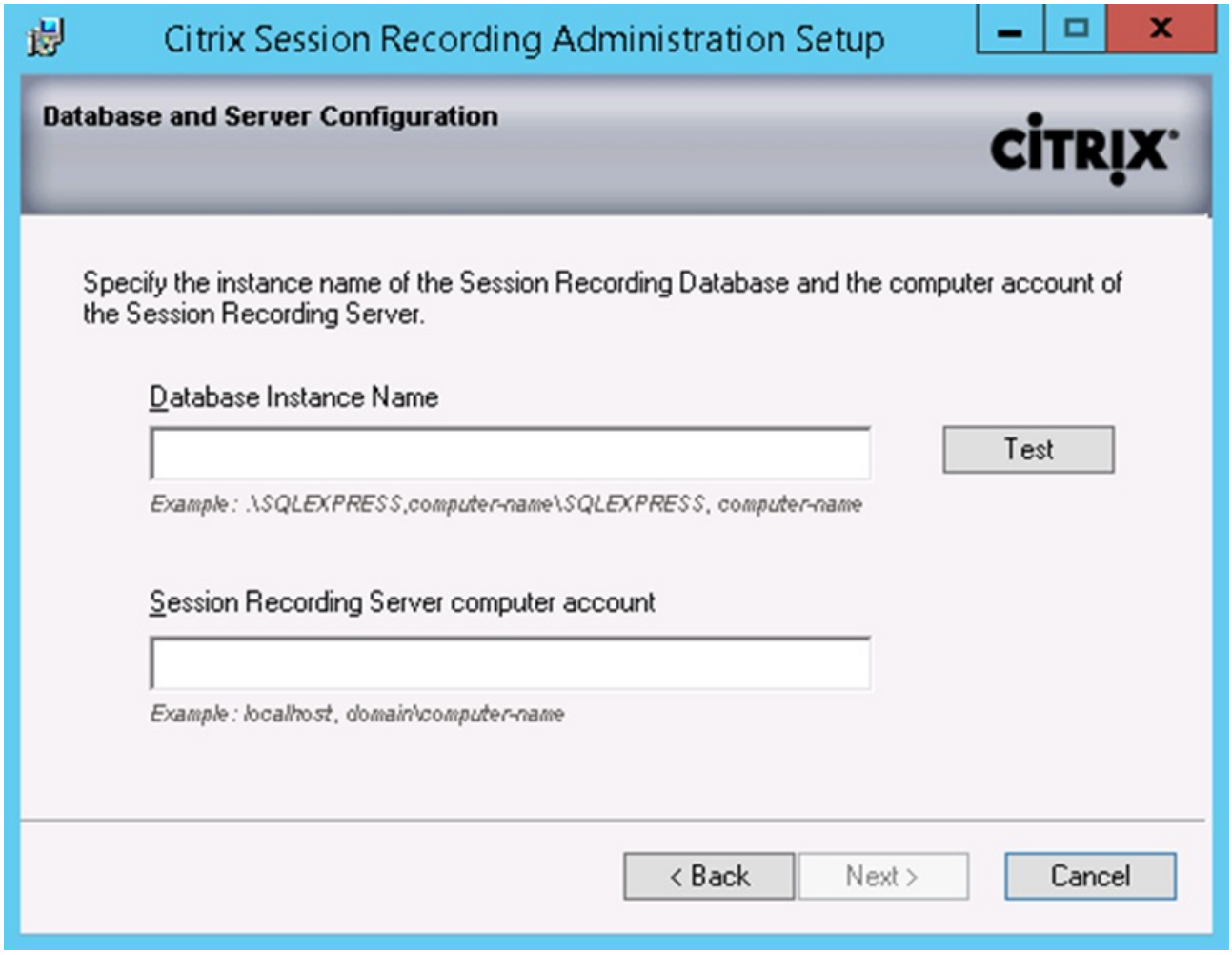
Stellen Sie sicher, dass alle Voraussetzungen installiert sind, bevor Sie die Datenbank für die Sitzungsaufzeichnung installieren. Weitere Informationen finden Sie unter Systemanforderungen für die Sitzungsaufzeichnung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

In der Regel werden die Datenbank der Sitzungsaufzeichnung und Microsoft SQL Server auf eine von dreierlei Weisen bereitgestellt:

- Bereitstellung 1: Installation des Sitzungsaufzeichnungsservers und der Datenbank für die Sitzungsaufzeichnung auf demselben Server und Installation von Microsoft SQL Server auf einer Remotemaschine (**empfohlen**)
- Bereitstellung 2: Installation des Sitzungsaufzeichnungsservers, der Datenbank für die Sitzungsaufzeichnung und von Microsoft SQL Server auf derselben Maschine
- Bereitstellung 3: Installation des Sitzungsaufzeichnungsservers auf einem Server und Installation der Datenbank für die Sitzungsaufzeichnung sowie von Microsoft SQL Server zusammen auf einer anderen Maschine (**nicht empfohlen**)

1. Auf der Seite zur Konfiguration der Datenbank:
   - **Bereitstellung 1 und 2:** Geben Sie in dem Feld für das Computerkonto des Sitzungsaufzeichnungsservers **localhost** ein.
   - **Bereitstellung 3**: Geben Sie den Namen des Computers, der den Sitzungsaufzeichnungsserver hostet, in folgendem Format ein: *Domäne**Computername*. Das Computerkonto des Sitzungsaufzeichnungsservers wird als Benutzerkonto für den Zugriff auf die Datenbank verwendet.




Wenn die Datenbankinstanz keine benannte Instanz ist, die Sie beim Setup der Instanz konfiguriert haben, können Sie nur den Computernamen des SQL Server-Computers verwenden. Wenn Sie die Instanz benannt haben, verwenden Sie *Computername**Instanzname* als Datenbankinstanznamen. Um den verwendeten Servernamen zu ermitteln, führen Sie **select @@servername** auf dem SQL Server-Computer aus. Der zurückgegebene Name ist der Datenbankinstanzname.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf **Test**, um die Verbindung mit dem SQL Server-Computer zu testen. Stellen Sie sicher, dass der aktuelle Benutzer die öffentliche SQL Server-Rollenberechtigung hat, ansonsten schlägt der Test aufgrund einer fehlenden Berechtigung fehl. Klicken Sie auf **Weiter**, um die Installation fortzusetzen.

2. Befolgen Sie die Anweisungen zum Abschließen der Installation. Wenn der aktuelle Benutzer nicht der Datenbankadministrator ist, wird während der Installation ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit der sysadmin-Serverrollenberechtigung eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um die Installation fortzusetzen. Es wird eine neue Datenbank für die Sitzungsaufzeichnung erstellt und das Maschinenkonto des Sitzungsaufzeichnungsservers wird als **db-owner** hinzugefügt.

Nach Abschluss der Installation wird die sysadmin-Serverrollenberechtigung nicht mehr benötigt und kann für den aktuellen Benutzer entfernt werden.

> **Important**
>
> Sie können den Datenbanknamen **CitrixSessionRecording** nicht ändern.

### Installieren des Sitzungsaufzeichnungsservers

Stellen Sie sicher, dass alle Voraussetzungen installiert sind, bevor Sie den Sitzungsaufzeichnungsserver installieren. Weitere Informationen finden Sie unter Systemanforderungen für die Sitzungsaufzeichnung.

1. Geben Sie den Namen des SQL-Servers im Textfeld "Datenbankinstanzname" ein. Wenn Sie eine benannte Instanz verwenden, geben Sie *Computername**Instanzname* ein, andernfalls geben Sie nur einen Computernamen ein.
2. Klicken Sie auf **Test**, um die Verbindung mit dem SQL-Server zu testen. Stellen Sie sicher, dass der aktuelle Benutzer die öffentliche SQL Server-Rollenberechtigung hat, ansonsten schlägt der Test aufgrund einer fehlenden Berechtigung fehl. Klicken Sie dann auf **Weiter** und folgen Sie den Anweisungen, um die Installation abzuschließen.
3. Am Ende des Installations-Assistenten können Sie entscheiden, ob Sie sich an dem Programm zur Verbesserung der Benutzerfreundlichkeit von Citrix beteiligen möchten. Wenn Sie diesem Programm beitreten, werden anonyme Statistik- und Nutzungsinformationen an Citrix gesendet. Weitere Informationen finden Sie unter Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP).

Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers

Sie können mit der Director-Konsole Sitzungsaufzeichnungsrichtlinien erstellen und aktivieren.

1. Zur Verwendung einer HTTPS-Verbindung installieren Sie das Zertifikat zum Vertrauen des Sitzungsaufzeichnungsservers im Ordner mit den vertrauenswürdigen Stammzertifikaten des Director-Servers.
2. Zum Konfigurieren des Director-Servers für die Verwendung des Sitzungsaufzeichnungsservers führen Sie den Befehl **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording** aus.
3. Geben Sie die IP-Adresse bzw. den FQDN des Sitzungsaufzeichnungsservers, die Portnummer und den Verbindungstyp (http/https) für die Verbindung zwischen Sitzungsaufzeichnungsagent und Sitzungsaufzeichnungsbroker auf dem Director-Server ein.

### Installieren des Sitzungsaufzeichnungsagents

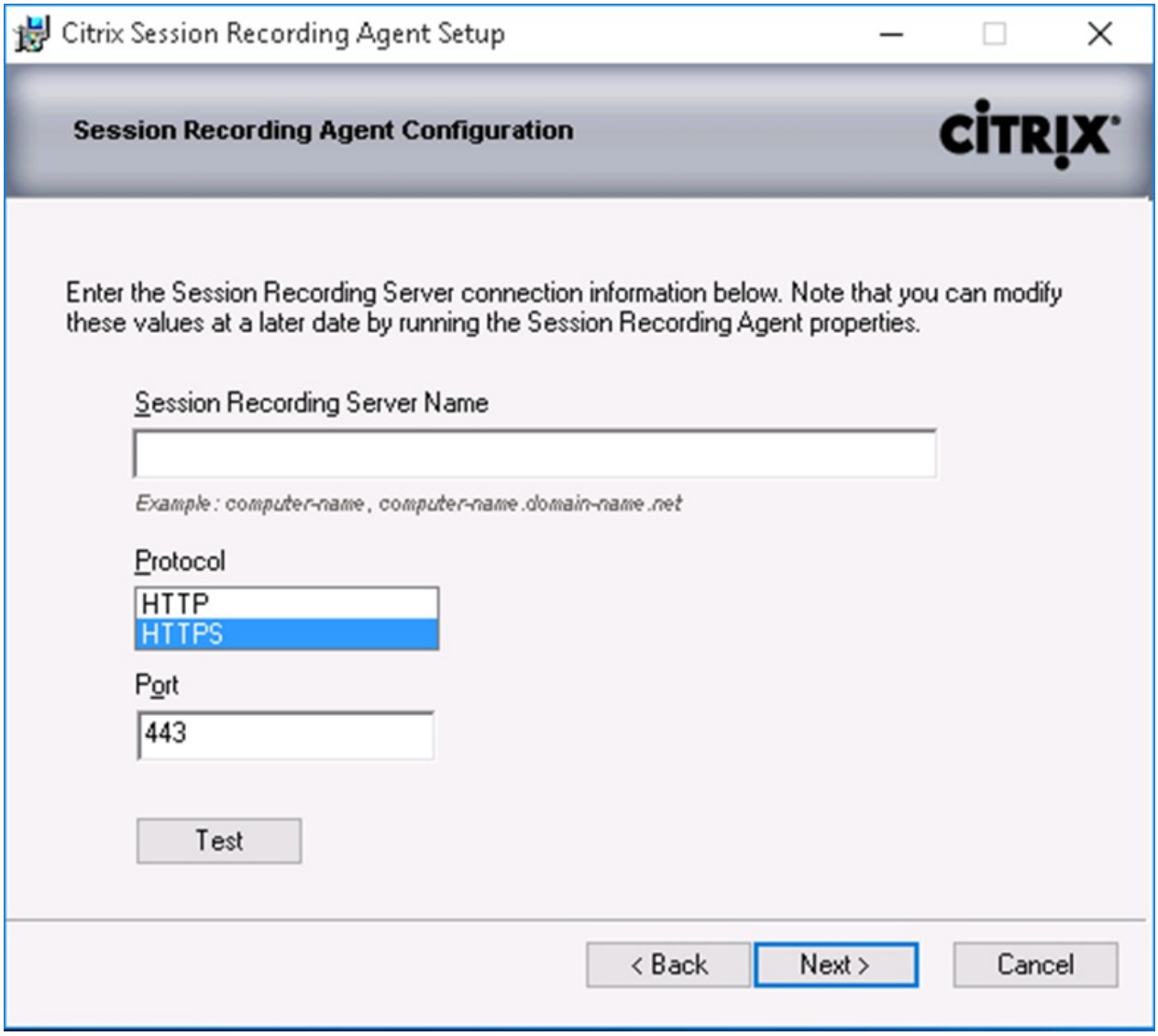
Installieren Sie den Sitzungsaufzeichnungsagent auf der Serverbetriebssystem-VDA bzw. -VDI-Maschine, auf der Sie Sitzungen aufzeichnen möchten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Installieren Sie unter Verwendung des Server-Managers auf dem XenApp 7.8-Serverbetriebssystem-VDA bzw. dem XenDesktop 7.8-VDI .NET Framework 3.5 und Microsoft Message Queuing (MSMQ) mit HTTP-Unterstützung.
2. Starten Sie die Windows-Eingabeaufforderung als Administrator und führen Sie den folgenden Befehl aus:
   **msiexec /i SessionRecordingAgentx64.msi**
   oder
   **msiexec /i SessionRecordingAgent.msi**

   oder doppelklicken Sie auf die MSI-Datei.

   Verwenden Sie jeweils die für die Plattform vorgesehene MSI-Datei: **SessionRecordingAgent.msi** für 32-Bit-Systeme und **SessionRecordingAgentx64.msi** für 64-Bit-Systeme.
3. Klicken Sie im Installationsprogramm auf **Weiter** und akzeptieren Sie die Lizenzvereinbarung.
4. Geben Sie auf der Seite "Sitzungsaufzeichnungsagent - Konfiguration" den Namen des Computers ein, auf dem Sie den Sitzungsaufzeichnungsserver installiert haben, sowie das Protokoll und die Portinformationen für die Verbindung mit dem Sitzungsaufzeichnungsserver.




Standardmäßig verwendet die Sitzungsaufzeichnung HTTPS/TLS für die sichere Kommunikation. Wenn TLS nicht


© 1999-2017 Citrix Systems, Inc. All rights reserved.

konfiguriert ist, verwenden Sie HTTP. Navigieren Sie dazu zur Sitzungsaufzeichnungsbroker-Site und deaktivieren Sie SSL in der IIS-Verwaltungskonsole. Öffnen Sie die SSL-Einstellungen und deaktivieren Sie das Kontrollkästchen "SSL erfordern".

5. Befolgen Sie die Anweisungen zum Abschließen der Installation.

### Installieren des Sitzungsaufzeichnungsplayers

Installieren Sie den Sitzungsaufzeichnungsplayer auf dem Sitzungsaufzeichnungsserver oder auf mindestens einer Arbeitsstation in der Domäne für Benutzer, die Sitzungsaufzeichnungen anzeigen.

Führen Sie **SessionRecordingPlayer.msi** aus und folgen Sie den Anweisungen zum Durchführen der Installation.

### Automatisieren der Installationen

Zur Installation des Sitzungsaufzeichnungsagents auf mehreren Servern können Sie ein Skript erstellen, das eine Installation ohne Benutzereingriffe ausführt.

Mit der folgenden Befehlszeile installieren Sie den Sitzungsaufzeichnungsagent und erstellen eine Protokolldatei, in der die Installationsinformationen aufgezeichnet werden.

**64-Bit-Systeme:**

```
msiexec /i SessionRecordingAgentx64.msi
sessionrecordingservername=yourservername sessionrecordingbrokerprotoco=yourbrokerprotocol
 sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q
```

**32-Bit-Systeme:**

```
msiexec /i  SessionRecordingAgent.msi sessionrecordingservername=yourservername
sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /l*v yourinstallationlog /q
```

Wobei Folgendes gilt:

*yourservername* ist der NetBIOS-Name oder FQDN des Computers, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird. Wenn Sie keinen Namen eingeben, wird der Standardwert "localhost" verwendet.

*yourbrokerprotocol* (HTTP oder HTTPS) ist das Protokoll, mit dem der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Wenn Sie keine Eingabe machen, wird als Standardwert HTTPS verwendet.

*yourbrokerport* ist eine Ganzzahl, die den Port angibt, über den der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Wenn Sie keine Eingabe machen, wird als Standardwert 0 verwendet, d. h. der Sitzungsaufzeichnungsagent verwendet den Standardport für das ausgewählte Protokoll: 80 für HTTP oder 443 für HTTPS.

**/l*v** gibt eine ausführliche Protokollierung an.

*yourinstallationlog* ist der Speicherort, an dem die Setupprotokolldatei erstellt wird.

**/q** gibt den stillen Modus an.

### Upgrade der Sitzungsaufzeichnung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Sie können ein Upgrade von Version 7.6.0 (oder einer höheren Version) der Sitzungsaufzeichnung auf die neueste freigegebene

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

(aktuelle) Version durchführen.

Anforderungen, Vorbereitung und Einschränkungen

**Hinweis:** Sie können kein Upgrade von einer Technology Preview-Version ausführen.

- Sie müssen über die grafische Oberfläche oder die Befehlszeile des Installationsprogramms für die Sitzungsaufzeichnung ein Upgrade von deren Komponenten auf der Maschine ausführen, auf der die Komponenten installiert sind.
- Vor Beginn des Upgrades sichern Sie die Datenbank "CitrixSessionRecording" auf der SQL Server-Instanz, damit Sie sie im Falle eines Problems nach dem Datenbankupgrade wiederherstellen können.
- Auf den Maschinen, auf denen Sie die Komponenten der Sitzungsaufzeichnung aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.
- Sind Server und Datenbank der Sitzungsaufzeichnung nicht auf dem gleichen Server installiert, benötigen Sie die Datenbank-sysadmin-Rollenberechtigung für das Upgrade der Datenbank für die Sitzungsaufzeichnung. Ansonsten werden Sie während des Upgrades zum Eingeben der Anmeldeinformationen für die sysadmin-Rolle aufgefordert.
- Wenn Sie nicht alle Sitzungsaufzeichnungsagents zur gleichen Zeit aktualisieren möchten, können Sie Version 7.6.0 (oder höher) für die aktuelle Version des Sitzungsaufzeichnungsservers verwenden. Allerdings stehen dann einige neue Features und Fehlerbehebungen ggf. nicht zur Verfügung.
- Sitzungen, die während des Upgrades des Sitzungsaufzeichnungsservers gestartet werden, werden nicht aufgezeichnet.
- Bei zu Beginn des Upgrades laufenden Sitzungen besteht ein geringes Risiko, dass deren Aufzeichnung nicht ausgeführt werden kann.
- Lesen Sie den Abschnitt zur Upgradereihenfolge weiter unten, damit Sie mögliche Ausfälle einplanen und das Risiko senken können.

Aktualisierungsreihenfolge

1. Sind Server und Datenbank der Sitzungsaufzeichnung auf verschiedenen Servern installiert, beenden Sie den Speichermanager der Sitzungsaufzeichnung auf dem Sitzungsaufzeichnungsserver manuell und führen Sie zunächst das Upgrade der Datenbank durch.
2. Stellen Sie sicher, dass der Sitzungsaufzeichnungsbroker mit IIS ausgeführt wird. Führen Sie das Upgrade des Sitzungsaufzeichnungsservers durch. Sind Datenbank und Server der Sitzungsaufzeichnung auf dem gleichen Server installiert, erfolgt auch ein Upgrade der Datenbank.
3. Der Sitzungsaufzeichnungsdienst geht automatisch wieder online, sobald das Upgrade des Sitzungsaufzeichnungsserver abgeschlossen ist.
4. Führen Sie das Upgrade des Sitzungsaufzeichnungsagents (auf dem Masterimage) durch.
5. Führen Sie das Upgrade der Richtlinienkonsole für die Sitzungsaufzeichnung zusammen mit oder nach dem des Sitzungsaufzeichnungsservers durch.
6. Führen Sie das Upgrade des Sitzungsaufzeichnungsplayers durch.

## Deinstallieren der Sitzungsaufzeichnung

Sie entfernen Komponenten der Sitzungsaufzeichnung von einem Server oder einer Arbeitsstation über die Option zum Deinstallieren von Programmen in der Windows-Systemsteuerung. Zum Entfernen der Datenbank für die Sitzungsaufzeichnung benötigen Sie die gleiche SQL Server-Rollenberechtigung sysadmin wie bei der Installation.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Skripts zum Hinzufügen erforderlicher Windows-Rollen und -Features

Jul 08, 2016

Mit den folgenden Skripts können Sie die Windows-Rollen und -Features installieren, die für die ordnungsgemäße Ausführung der Sitzungsaufzeichnung erforderlich sind. Weitere Informationen finden Sie unter Hinzufügen erforderlicher Windows-Rollen und Features mit einem Skript.

Installieren von Voraussetzungen für die Verwaltung der Sitzungsaufzeichnung KOPIEREN

```
<#
.Synopsis
    Installs Prereqs for Session Recording Administration
.Description
    Supports Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.
    Install below windows feature on this machine:
    -Application Development - ASP.NET 4.5 on Server 2012 and Server 2012 R2, Application Development - ASP.NET on Server 2008 R2
    -Security - Windows Authentication
    -Management Tools - IIS 6 Management Compatibility
        IIS 6 Metabase Compatibility
        IIS 6 WMI Compatibility
        IIS 6 Scripting Tools
        IIS 6 Management Console
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.
#>
function AddFeatures($featurename)
{
    try
    {
        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        Add-WindowsFeature $feature
    }
    catch
    {
        Write-Host "Addition of Windows feature $featurename failed"
        Exit 1
    }
    Write-Host "Addition of Windows feature $featurename succeeded"
}

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')))
{
    Write-Host("This is not a supported server platform. Installation aborted.")
    Exit
}

# Start to install Windows feature
Import-Module ServerManager

if ($system -Like '*Microsoft Windows Server 2012*')
{
    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
}
if($system -like '*Microsoft Windows Server 2008 R2*')
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    AddFeatures('Web-Asp-Net') #ASP.NET
}
AddFeatures('Web-Mgmt-Console') #IIS Management Console
AddFeatures('Web-Windows-Auth') # Windows Authentication
AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
```

Installieren von Voraussetzungen für den Sitzungsaufzeichnungsagent

KOPIEREN

```
<#
.Synopsis
    Installs Prereqs for Session Recording Administration
.Description
    Supports Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8, Windows 8.1 and Windo
    Install below windows feature on this machine:
 -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.
#>
function AddFeatures($featurename)
{
    try
    {
        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        Add-WindowsFeature $feature

    }

    catch

    {

        Write-Host "Addition of Windows feature $featurename failed"

        Exit 1

    }

    Write-Host "Addition of Windows feature $featurename succeeded"

}



# Start to install Windows feature

$system= gwmi win32_operatingSystem | select name



if (-not (($system -Like '*Microsoft Windows Server 2012*') -or ($system -Like '*Microsoft Windows Server 2008 R2*')-or ($system -Like '*

{

    Write-Host("This is not a supported platform. Installation aborted.")

    Exit

}



if ($system -Like '*Microsoft Windows Server*')

{

    Import-Module ServerManager

    AddFeatures('MSMQ') #Message Queuing

    AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support

}

else

{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    try
    {
        if($system -Like '*Microsoft Windows 7*')
        {
            dism /online /enable-feature /featurename:IIS-WebServerRole /featurename:IIS-WebServer /featurename:IIS-IIS6ManagementCo
            dism /online /enable-feature /featurename:MSMQ-Container
            dism /online /enable-feature /featurename:MSMQ-Server
            dism /online /enable-feature /featurename:MSMQ-HTTP
        }
        else
        {
            dism /online /enable-feature /featurename:MSMQ-HTTP /all
        }
    }
    catch
    {
        Write-Host "Addition of Windows feature MSMQ HTTP Support failed"
        Exit 1
    }
    write-Host "Addition of Windows feature MSMQ HTTP Support succeeded"
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren der Sitzungsaufzeichnung

Jul 08, 2016

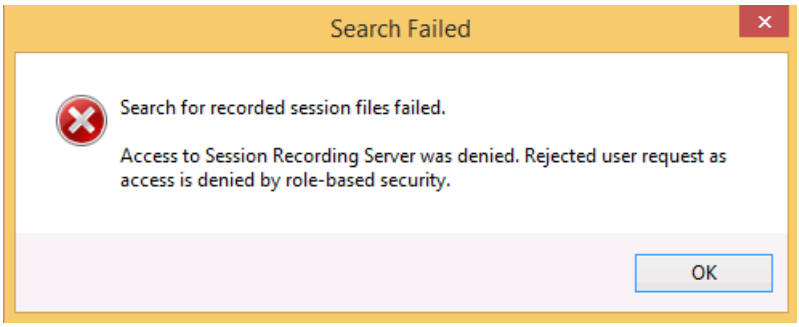
Konfigurieren der Sitzungsaufzeichnung für die Wiedergabe und Aufzeichnung von Sitzungen

Nach der Installation der Sitzungsaufzeichnungskomponenten konfigurieren Sie die Sitzungsaufzeichnung mit den folgenden Schritten für die Aufzeichnung von XenApp- bzw. XenDesktop-Sitzungen und das benutzerseitige Anzeigen der Sitzungen.

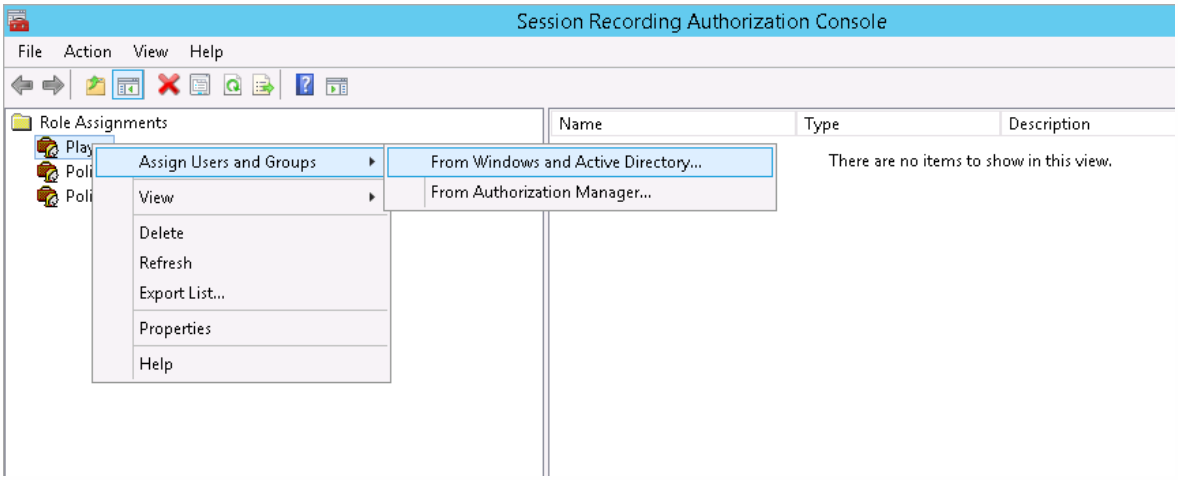
- Berechtigen von Benutzern zur Wiedergabe von Aufzeichnungen
- Berechtigen von Benutzern zur Verwaltung von Aufzeichnungsrichtlinien
- Festlegen der aktiven Aufzeichnungsrichtlinie zum Aufzeichnen von Sitzungen
- Konfigurieren von benutzerdefinierten Richtlinien
- Konfigurieren des Sitzungsaufzeichnungsplayers für die Verbindung mit dem Sitzungsaufzeichnungsserver

## Berechtigen von Benutzern zur Wiedergabe von Sitzungsaufzeichnungen

Nach der Installation der Sitzungsaufzeichnung ist zunächst kein Benutzer berechtigt, Sitzungsaufzeichnungen wiederzugeben. Sie müssen jedem Benutzer, einschließlich des Administrators, Berechtigungen zuweisen. Ein Benutzer ohne Berechtigung zur Wiedergabe von Sitzungsaufzeichnungen erhält die folgende Fehlermeldung bei dem Versuch, eine Sitzungsaufzeichnung wiederzugeben:




1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver als Administrator an.
2. Starten Sie die Sitzungsaufzeichnungsautorisierungskonsole.
3. Klicken Sie in der Sitzungsaufzeichnungsautorisierungskonsole auf Player.
4. Wählen Sie die Benutzer und Gruppen aus, denen Sie Berechtigungen zur Wiedergabe von Sitzungsaufzeichnungen geben möchten. Sie werden daraufhin im rechten Bereich angezeigt.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Berechtigen von Benutzern zur Verwaltung von Aufzeichnungsrichtlinien

Bei der Installation der Sitzungsaufzeichnung gewähren standardmäßig Domänenadministratoren Berechtigung zum Steuern von Aufzeichnungsrichtlinien. Sie können die Autorisierungseinstellung ändern.

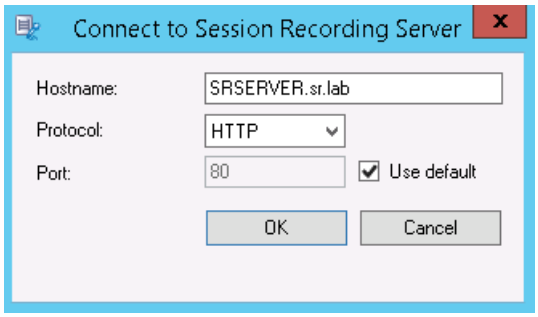
1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver als Administrator an.
2. Starten Sie die Sitzungsaufzeichnungsautorisierungskonsole und wählen Sie PolicyAdministrators aus.
3. Fügen Sie die Benutzer und Gruppen hinzu, die Aufzeichnungsrichtlinien verwalten sollen.

## Festlegen der aktiven Aufzeichnungsrichtlinie zum Aufzeichnen von Sitzungen

Die aktive Aufzeichnungsrichtlinie legt das Sitzungsaufzeichnungsverhalten für alle VDAs und VDIs fest, auf denen der Sitzungsaufzeichnungsagent installiert ist und die eine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen. Bei der Installation der Sitzungsaufzeichnung wird als aktive Richtlinie **Nicht aufzeichnen** verwendet. Sitzungen können erst aufgezeichnet werden, wenn Sie die aktive Aufzeichnungsrichtlinie ändern.

**Wichtig:** Eine Richtlinie kann viele Regeln enthalten, aber es kann jeweils nur eine aktive Richtlinie ausgeführt werden.

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld Mit Sitzungsaufzeichnungsserver verbinden angezeigt wird, stellen Sie sicher, dass der Name des Computers, auf dem der Sitzungsaufzeichnungsserver gehostet wird, das Protokoll und der Port richtig sind.




4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung Aufzeichnungsrichtlinien. Die bei der Installation der Sitzungsaufzeichnung erstellten Aufzeichnungsrichtlinien werden angezeigt. Ein Häkchen gibt die aktive Richtlinie an:
   - Nicht aufzeichnen: Die Standardrichtlinie. Wenn Sie keine andere Richtlinie festlegen, wird keine Sitzung aufgezeichnet.
   - Alle mit Benachrichtigung aufzeichnen: Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Der Benutzer wird in einem Popupfenster über die Aufzeichnung informiert.
   - Alle ohne Benachrichtigung aufzeichnen: Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Der Benutzer wird nicht in einem Popupfenster über die Aufzeichnung informiert.
5. Wählen Sie die Richtlinie aus, die Sie als aktive Richtlinie verwenden möchten.
6. Klicken Sie im Menü auf Aktion > Richtlinie aktivieren.

Hinweis: Sie können in der Sitzungsaufzeichnung eigene Aufzeichnungsrichtlinien erstellen. Die erstellten Aufzeichnungsrichtlinien werden im Ordner "Aufzeichnungsrichtlinien" in der Richtlinienkonsole für die Sitzungsaufzeichnung angezeigt.
Die generische Aufzeichnungsrichtlinie entspricht u. U. nicht Ihren Anforderungen. Sie können Richtlinien und Regeln basierend auf Benutzern, VDA- und VDI-Servern, Bereitstellungsgruppen und Anwendungen konfigurieren. Weitere Informationen zu benutzerdefinierten Richtlinien finden Sie unter Erstellen benutzerdefinierter Aufzeichnungsrichtlinien.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren des Sitzungsaufzeichnungsplayers

Damit der Sitzungsaufzeichnungsplayer Sitzungen wiedergeben kann, müssen Sie die Verbindung mit dem Sitzungsaufzeichnungsserver konfigurieren, auf dem die Sitzungsaufzeichnungen gespeichert sind. Jeder Sitzungsaufzeichnungsplayer kann eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen, jedoch kann nur jeweils eine Verbindung aktiv sein. Wenn ein Sitzungsaufzeichnungsplayer eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, können Benutzer den gewünschten Sitzungsaufzeichnungsserver durch Auswahl eines Kontrollkästchens auf der Registerkarte **Verbindungen** unter **Extras > Optionen** festlegen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Starten Sie den Sitzungsaufzeichnungsplayer.
3. Wählen Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers Extras > Optionen aus.
4. Klicken Sie auf der Registerkarte Verbindungen auf Hinzufügen.
5. Geben Sie im Feld Hostname den Namen oder die IP-Adresse des Computers mit dem Sitzungsaufzeichnungsserver ein und wählen Sie das Protokoll aus. Standardmäßig verwendet die Sitzungsaufzeichnung HTTPS/SSL für die sichere Kommunikation. Wenn SSL nicht konfiguriert ist, wählen Sie "HTTP".
6. Wenn der Sitzungsaufzeichnungsplayer eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, wiederholen Sie Schritt 4 und 5 für jeden Server.
7. Stellen Sie sicher, dass das Kontrollkästchen für den Sitzungsaufzeichnungsserver aktiviert ist, mit dem Sie eine Verbindung herstellen möchten.

## Konfigurieren der Verbindung mit dem Sitzungsaufzeichnungsserver

Die Verbindung zwischen Sitzungsaufzeichnungsagent und dem Sitzungsaufzeichnungsserver wird normalerweise bei der Installation des Agents konfiguriert. Die Verbindung kann nach der Installation des Sitzungsaufzeichnungsagents in dessen Eigenschaften konfiguriert werden.

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Verbindungen**.
4. Geben Sie im Feld **Sitzungsaufzeichnungsserver** den Namen oder die IP-Adresse des Servers ein.
5. Wählen Sie im Bereich **Nachrichtenwarteschlange des Speichermanagers der Sitzungsaufzeichnung** das Protokoll aus, das der Speichermanager der Sitzungsaufzeichnung für die Kommunikation verwendet. Sie können auch die Standardportnummer ändern.
6. Akzeptieren Sie im Feld **Nachrichtenlebensdauer** den Standard von 7200 Sekunden (zwei Stunden) oder geben Sie einen neuen Wert für die Zeit in Sekunden ein, für die jede Nachricht in der Warteschlange gespeichert wird, wenn ein Kommunikationsfehler auftritt. Nach dem Ablauf dieses Zeitraums wird die Nachricht gelöscht und die Datei kann nur bis an die Stelle wiedergegeben werden, an der die Daten verloren wurden.
7. Wählen Sie im Bereich **Sitzungsaufzeichnungsbroker** das Protokoll aus, das der Sitzungsaufzeichnungsbroker für die Kommunikation verwendet. Sie können auch die Standardportnummer ändern.
8. Starten Sie den Sitzungsaufzeichnungsagent-Dienst neu, um die Änderung zu übernehmen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Gewähren von Zugriffsrechten für Benutzer

Jul 08, 2016

Hinweis: Aus Sicherheitsgründen sollten Sie den Benutzern nur die Rechte geben, die sie zum Ausführen bestimmter Funktionen benötigen, z. B. zum Anzeigen aufgezeichneter Sitzungen.

Sie weisen den Benutzern in der Sitzungsaufzeichnungsautorisierungskonsole auf dem Sitzungsaufzeichnungsserver Rollen zu und gewähren den Sitzungsaufzeichnungsbenutzern Rechte. Sitzungsaufzeichnungsbenutzer haben drei Rollen:

- **Player:** Mitglieder der Rolle können aufgezeichnete XenApp-Sitzungen anzeigen. Für diese Rolle besteht keine Standardeinstellung.
- **PolicyQuery:** Die Server mit dem Sitzungsaufzeichnungsagent können Auswertungen der Aufzeichnungsrichtlinie anfordern. In der Standardeinstellung sind authentifizierte Benutzer Mitglieder dieser Rolle.
- **PolicyAdministrator:** Mitglieder dieser Rolle können Aufzeichnungsrichtlinien anzeigen, erstellen, bearbeiten, löschen und aktivieren. In der Standardeinstellung sind Administratoren des Computers, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird, Mitglieder dieser Rolle.

Die Sitzungsaufzeichnung unterstützt in Active Directory definierte Benutzer und Gruppen.

## Zuweisen von Rollen zu Benutzern

1. Melden Sie sich bei dem Computer, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird, als Administrator oder Richtlinienadministrator an.
2. Starten Sie die Sitzungsaufzeichnungs-Autorisierungskonsole.
3. Wählen Sie die Rolle, der Sie Benutzer zuordnen möchten.
4. Wählen Sie auf der Menüleiste Aktion > Windows-Benutzer und -Gruppen zuweisen.
5. Fügen Sie die Benutzer und Gruppen hinzu.

In der Konsole vorgenommene Änderungen werden beim Update (das jede Minute erfolgt) übernommen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen und Aktivieren von Aufzeichnungsrichtlinien

Jul 08, 2016

Mit der Richtlinienkonsole für die Sitzungsaufzeichnung erstellen und aktivieren Sie Richtlinien, die festlegen, wie Sitzungen aufgezeichnet werden.

Sie können verfügbare Systemrichtlinien nach der Installation der Sitzungsaufzeichnung aktivieren oder eigene Richtlinien erstellen und aktivieren. Die Systemrichtlinien für die Sitzungsaufzeichnung wenden eine Regel auf alle Benutzer, veröffentlichten Anwendungen und Server an. In benutzerdefinierten Richtlinien geben Sie an, welche Benutzer, veröffentlichten Anwendungen und Server aufgezeichnet werden.

Die aktive Richtlinie legt fest, welche Sitzungen aufgezeichnet werden. Nur jeweils eine Richtlinie ist aktiv.

## Verwenden von Systemrichtlinien

Die Sitzungsaufzeichnung enthält die folgenden Systemrichtlinien:

- **Nicht aufzeichnen**: Bei Auswahl dieser Richtlinie werden keine Sitzungen aufgezeichnet. Dies ist die Standardrichtlinie. Wenn Sie keine andere Richtlinie angeben, werden keine Sitzungen aufgezeichnet.
- **Alle mit Benachrichtigung aufzeichnen**: Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Der Benutzer wird in einem Popupfenster über die Aufzeichnung informiert.
- **Alle ohne Benachrichtigung aufzeichnen**: Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Der Benutzer wird nicht in einem Popupfenster über die Aufzeichnung informiert.

Systemrichtlinien können nicht geändert oder gelöscht werden.

## Aktivieren einer Richtlinie

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld Mit Sitzungsaufzeichnungsserver verbinden angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf OK.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung Aufzeichnungsrichtlinien.
5. Wählen Sie die Richtlinie aus, die Sie als aktive Richtlinie verwenden möchten.
6. Klicken Sie im Menü auf Aktion > Richtlinie aktivieren.

## Erstellen benutzerdefinierter Aufzeichnungsrichtlinien

Wenn Sie eine eigene Richtlinie erstellen, legen Sie Regeln fest und geben an, welche Sitzungen von Benutzern und Gruppen, veröffentlichten Anwendungen und Servern aufgezeichnet werden. Ein Assistent in der Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt Sie beim Erstellen der Regeln. Zum Abrufen einer Liste der veröffentlichten Anwendungen und Server ist Siteadministrator-Leseberechtigung erforderlich. Konfigurieren Sie dies auf dem Delivery Controller der Site.

Für jede erstellte Regel geben Sie eine Aufzeichnungsaktion und ein Regelkriterium an. Die Aufzeichnungsaktion gilt für Sitzungen, die das Regelkriterium erfüllen.

Wählen Sie für jede Regel eine Aufzeichnungsaktion aus:

- Nicht aufzeichnen: (Wählen Sie Sitzungsaufzeichnung deaktivieren im Assistenten für Regeln.) Diese


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, nicht aufgezeichnet werden.

- Mit Benachrichtigung aufzeichnen: (Wählen Sie Sitzungsaufzeichnung mit Benachrichtigung aktivieren im Assistenten für Regeln.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, nicht aufgezeichnet werden. Der Benutzer wird in einem Popupfenster über die Aufzeichnung informiert.
- Ohne Benachrichtigung aufzeichnen: (Wählen Sie Sitzungsaufzeichnung ohne Benachrichtigung aktivieren im Assistenten für Regeln.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, nicht aufgezeichnet werden. Benutzer werden nicht über die Aufzeichnung informiert.

Wählen Sie für jede Regel mindestens eines der folgenden Elemente, um ein Regelkriterium zu erstellen:

- Benutzer oder Gruppen: Sie erstellen eine Liste der Benutzer oder Gruppen, für die die Aufzeichnungsaktion der Regel gilt.
- Veröffentlichte Ressourcen: Sie erstellen eine Liste der veröffentlichten Anwendungen oder Desktops, auf die die Aufzeichnungsaktion der Regel angewendet wird. Wählen Sie im Assistenten für Regeln die XenApp-/XenDesktop-Sites aus, auf denen die Anwendungen bzw. Desktops verfügbar sind.
- Bereitstellungsgruppen oder Maschinen: Sie erstellen eine Liste der Bereitstellungsgruppen oder Maschinen, auf die die Aufzeichnungsaktion der Regel angewendet wird. Wählen Sie im Assistenten für Regeln den Speicherort, an dem die Bereitstellungsgruppen oder Maschinen residieren.

Wenn Sie mehrere Regeln in einer Aufzeichnungsrichtlinie erstellen, können einige Sitzungen die Kriterien für mehrere Regeln erfüllen. In diesen Situationen wird die Regel mit der höchsten Priorität auf die Sitzung angewendet.

Die Aufzeichnungsaktion einer Regel legt die Priorität fest:

- Regeln mit der Aktion Sitzungsaufzeichnung deaktivieren haben die höchste Priorität.
- Regeln mit der Aktion Sitzungsaufzeichnung mit Benachrichtigung aktivieren haben die nächsthöhere Priorität.
- Regeln mit der Aktion Sitzungsaufzeichnung ohne Benachrichtigung aktivieren haben die niedrigste Priorität.

Einige Sitzungen erfüllen ggf. kein Regelkriterium in einer Aufzeichnungsrichtlinie. Für diese Sitzungen gilt die Aufzeichnungsaktion der Fallbackregel der Richtlinie. Die Aufzeichnungsaktion der Fallbackregel ist immer Nicht aufzeichnen. Die Fallbackregel kann nicht geändert oder gelöscht werden.

**Konfigurieren von benutzerdefinierten Richtlinien**

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung und wählen Sie im linken Bereich **Aufzeichnungsrichtlinien** und in der Menüleiste **Aktion > Neue Richtlinie hinzufügen**.
3. Klicken Sie mit der rechten Maustaste auf **Neue Richtlinie** und wählen Sie **Neue Regel hinzufügen**.
4. **Aufzeichnungsoption wählen:** Wählen Sie im Regelassistenten die Option **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** (oder "ohne Benachrichtigung") und klicken Sie auf **Weiter**.
5. **Regelkriterien wählen:** Sie können eine beliebige Kombination der drei Optionen wählen:
   **Benutzer oder Gruppen**
   **Veröffentlichte Ressourcen**
   **Bereitstellungsgruppen oder Maschinen**
6. **Regelkriterium bearbeiten:** Klicken Sie zum Bearbeiten auf die unterstrichenen Werte. Welche Werte unterstrichen sind, hängt von den Kriterien ab, die Sie im vorherigen Schritt ausgewählt haben.
7. Folgen Sie dem Assistenten, um die Konfiguration abzuschließen.

**Verwenden von Active Directory-Gruppen**

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Beim Erstellen von Richtlinien können Sie in der Sitzungsaufzeichnung Active Directory-Gruppen verwenden. Active Directory-Gruppen statt einzelner Benutzer vereinfachen die Erstellung und Verwaltung von Regeln und Richtlinien. Beispiel: Wenn Benutzer in der Buchhaltungsabteilung des Unternehmens zur Active Directory-Gruppe "Finanz" gehören, können Sie eine Regel erstellen, die für alle Mitglieder dieser Gruppe gilt, indem Sie die Gruppe "Finanz" beim Erstellen der Regel im Assistenten für Regeln auswählen.

**Positivliste der Benutzer**

Sie können Richtlinien für die Sitzungsaufzeichnung erstellen, die sicherstellen, dass die Sitzungen bestimmter Benutzer im Unternehmen nie aufgezeichnet werden. Dies wird Positivliste der Benutzer genannt. Eine Positivliste der Benutzer ist beispielsweise für Benutzer geeignet, die mit vertraulichen Informationen arbeiten, oder in Situationen, in denen das Unternehmen die Sitzungen einer bestimmten Mitarbeitergruppe nicht aufzeichnen möchte.

Wenn beispielsweise alle Mitglieder der Geschäftsleitung im Unternehmen zu einer Active Directory-Gruppe "Geschäftsführung" gehören, können Sie sicherstellen, dass die Sitzungen dieser Benutzer nie aufgezeichnet werden, wenn Sie eine Regel erstellen, mit der die Sitzungsaufzeichnung für die Gruppe "Geschäftsführung" deaktiviert wird. Während die Richtlinie, die diese Regel enthält, aktiv ist, werden keine Sitzungen der Mitglieder der Gruppe "Geschäftsführung" aufgezeichnet. Die Sitzungen anderer Mitarbeiter im Unternehmen werden basierend auf den anderen Regeln in der aktiven Richtlinie aufgezeichnet.

**Erstellen einer Richtlinie**

Hinweis: Bei der Verwendung des Richtlinienassistenten werden Sie möglicherweise aufgefordert, zum Bearbeiten auf einen unterstrichenen Wert zu klicken, obwohl kein unterstrichener Wert angezeigt wird. Unterstrichene Werte werden nur in bestimmten Situationen angezeigt. Ignorieren Sie den Schritt, wenn kein unterstrichener Wert angezeigt wird.

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld Mit Sitzungsaufzeichnungsserver verbinden angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf OK.
4. Wählen Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung Aufzeichnungsrichtlinien.
5. Wählen Sie im Menü Neue Richtlinie hinzufügen. Im linken Bereich wird eine Neue Richtlinie genannte Richtlinie angezeigt.
6. Klicken Sie mit der rechten Maustaste auf die neue Richtlinie und wählen Sie im Menü Umbenennen.
7. Geben Sie einen Namen für die Richtlinie ein, die Sie erstellen, und drücken Sie die Eingabetaste oder klicken Sie außerhalb des neuen Namens.
8. Klicken Sie mit der rechten Maustaste auf die Richtlinie und starten Sie durch Auswahl von Neue Regel hinzufügen den Assistenten für Regeln.
9. Folgen Sie den Anweisungen, um die Regeln für diese Richtlinie zu erstellen.

**Ändern von Richtlinien**

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld Mit Sitzungsaufzeichnungsserver verbinden angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf OK.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung Aufzeichnungsrichtlinien.
5. Wählen Sie die Richtlinie aus, die Sie ändern möchten. Die Regeln für die Richtlinie werden im rechten Bereich angezeigt.
6. Fügen Sie eine Regel hinzu, ändern oder löschen eine Regel:
   - Klicken Sie auf der Menüleiste auf Aktion > Neue Regel hinzufügen. Wenn die Richtlinie aktiv ist, werden Sie in einem

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Popupfenster zum Bestätigen der Aktion aufgefordert. Erstellen Sie mit dem Assistenten für Regeln eine neue Regel.

- Markieren Sie die Regel, die Sie ändern möchten, klicken Sie mit der rechten Maustaste und wählen Sie Eigenschaften. Ändern Sie die Regel mit dem Assistenten für Regeln.
- Markieren Sie die Regel, die Sie löschen möchten, klicken Sie mit der rechten Maustaste und wählen Sie Regel löschen.

**Löschen von Richtlinien**

Hinweis: Eine Systemrichtlinie oder aktive Richtlinie kann nicht gelöscht werden.

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld Mit Sitzungsaufzeichnungsserver verbinden angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf OK.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung Aufzeichnungsrichtlinien.
5. Wählen Sie im linken Bereich die Richtlinie aus, die Sie löschen möchten. Wenn die Richtlinie aktiv ist, müssen Sie eine andere aktivieren.
6. Klicken Sie auf der Menüleiste auf Aktion > Richtlinie löschen.
7. Klicken Sie auf Ja, um die Aktion zu bestätigen.

## Grundlegendes zu Rollover

Wenn Sie eine Richtlinie aktivieren, bleibt die vorher aktive Richtlinie bis zum Ende der Benutzersitzung in Kraft. Manchmal wird die neue Richtlinie jedoch gültig, wenn ein Dateirollover erfolgt. Ein Dateirollover tritt auf, wenn das Limit für die maximale Größe erreicht wird. Weitere Informationen zur maximalen Dateigröße für Aufzeichnungen finden Sie unter Angeben der Dateigröße für Aufzeichnungen.

In der folgenden Tabelle werden die Vorgänge beschrieben, die beim Anwenden einer neuen Richtlinie auftreten, während eine Sitzung aufgezeichnet wird und ein Rollover erfolgt:

| Vorherige Richtlinie: | Neue Richtlinie: | Richtlinie nach Rollover: |
|---|---|---|
| Nicht aufzeichnen: | Jede andere Richtlinie | Keine Änderung. Die neue Richtlinie wird nur gültig, wenn sich der Benutzer an einer neuen Sitzung anmeldet. |
| Ohne Benachrichtigung aufzeichnen | Nicht aufzeichnen: | Aufzeichnung wird gestoppt. |
| | Mit Benachrichtigung aufzeichnen | Aufzeichnung wird fortgesetzt, und eine Benachrichtigung wird angezeigt. |
| Mit Benachrichtigung aufzeichnen | Nicht aufzeichnen: | Aufzeichnung wird gestoppt. |
| | Ohne Benachrichtigung aufzeichnen | Aufzeichnung wird fortgesetzt. Bei der nächsten Anmeldung des Benutzers wird keine Meldung angezeigt. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erstellen von Benachrichtigungen

Jul 08, 2016

Wenn in der aktiven Aufzeichnungsrichtlinie festgelegt ist, dass Benutzer über das Aufzeichnen der Sitzung benachrichtigt werden, wird ein Popupfenster mit einer Benachrichtigung angezeigt, nach dem die Benutzer die Anmeldeinformationen eingegeben haben. Die folgende Meldung ist die Standardbenachrichtigung: "Ihre Aktivität mit den von Ihnen vor kurzem gestarteten Programmen wird aufgezeichnet. Schließen Sie alle Programme, wenn Sie dies ablehnen." Der Benutzer klickt auf OK und setzt die Sitzung fort.

Die Standardbenachrichtigung wird in der Sprache des Betriebssystems des Computers angezeigt, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

Sie können benutzerdefinierte Benachrichtigungen in der gewünschten Sprache erstellen; jedoch ist nur eine Benachrichtigung pro Sprache möglich. Den Benutzern wird die Benachrichtigung in der Sprache angezeigt, die den lokalen Einstellungen des Benutzers entspricht.

## Erstellen einer neuen Benachrichtigung

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Benachrichtigungen.
4. Klicken Sie auf Hinzufügen.
5. Wählen Sie die Sprache für die Benachrichtigung und geben Sie den Text ein. Sie können nur eine Nachricht für jede Sprache erstellen.

Nach der Annahme und Aktivierung wird die neue Benachrichtigung im Feld Sprachspezifische Benachrichtigungen angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Deaktivieren oder Aktivieren der Aufzeichnung

Jul 08, 2016

Der Sitzungsaufzeichnungsagent wird auf jeder Serverbetriebssystemmaschine installiert, auf der Sie Sitzungen aufzeichnen möchten. Jeder Agent hat eine Einstellung, mit der die Aufzeichnung auf dem Server aktiviert wird, auf dem die Agentsoftware installiert ist. Nach dem Aktivieren der Aufzeichnung wertet die Sitzungsaufzeichnung die aktive Aufzeichnungsrichtlinie aus, mit der festgelegt wird, welche Sitzungen aufgezeichnet werden.

Bei Installation des Sitzungsaufzeichnungsagents ist die Aufzeichnung aktiviert. Citrix empfiehlt, dass Sie die Sitzungsaufzeichnung auf Servern deaktivieren, für die keine Aufzeichnung vorgesehen ist, da die Anwendung die Serverleistung geringfügig beeinträchtigt, selbst wenn keine Aufzeichnung erfolgt.

### Deaktivieren bzw. Aktivieren der Aufzeichnung auf einem Server

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf Sitzungsaufzeichnungsagent - Eigenschaften.
3. Aktivieren oder deaktivieren Sie unter Sitzungsaufzeichnung das Kontrollkästchen Sitzungsaufzeichnung für diesen XenApp-Server aktivieren, um anzugeben, ob Sitzungen für den Server aufgezeichnet werden sollen.
4. Starten Sie den Sitzungsaufzeichnungsagent-Dienst neu, um die Änderung zu übernehmen.

Hinweis: Bei der Installation der Sitzungsaufzeichnung wird als aktive Richtlinie Nicht aufzeichnen (auf keinem Server werden Sitzungen aufgezeichnet) verwendet. Aktivieren Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung eine andere Richtlinie, um die Aufzeichnung zu aktivieren.

# Aktivieren der Aufzeichnung benutzerdefinierter Ereignisse

In der Sitzungsaufzeichnung können Sie mit Anwendungen von Drittanbietern benutzerdefinierte Daten, so genannte Ereignisse, in die Sitzungsaufzeichnungen einfügen. Diese Ereignisse werden angezeigt, wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird. Die Ereignisse sind Teil der Sitzungsaufzeichnungsdatei und können nach dem Aufzeichnen der Sitzung nicht geändert werden.

Ein Ereignis kann beispielsweise den folgenden Text enthalten: Jedes Mal, wenn ein Benutzer einen Browser in einer Sitzung öffnet, die aufgezeichnet wird, wird der Text zu diesem Zeitpunkt in die Aufzeichnung eingefügt. Wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird, kann der Viewer anhand der Anzahl der Marker in der Liste "Ereignisse und Textmarken" im Player die Stellen suchen und zählen, an denen der Benutzer einen Browser geöffnet hat.

Einfügen benutzerdefinierter Ereignisse in Aufzeichnungen auf einem Server

- Aktivieren Sie über die Eigenschaften des Sitzungsaufzeichnungsagents eine Einstellung auf jedem Server, auf dem Sie benutzerdefinierte Ereignisse einfügen möchten. Sie müssen jeden Server einzeln aktivieren. Das globale Aktivieren aller Server in einer Site ist nicht möglich.
- Entwickeln Sie Anwendungen, die auf der Event-API basieren, die in der XenApp-Sitzung jedes Benutzers ausgeführt werden (zum Einfügen der Daten in die Aufzeichnung).

Bei der Installation der Sitzungsaufzeichnung wird auch eine Ereignisaufzeichnungs-COM-Anwendung (API) installiert, mit der Sie Text von Anwendungen von Drittherstellern in die Aufzeichnung einfügen können. Sie können die API von vielen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Programmiersprachen verwenden, u. a. Visual Basic, C++ oder C#. Die DLL-Datei der Sitzungsaufzeichnungs-Event-API ist Teil der Installation der Sitzungsaufzeichnung. Die Datei ist unter C:\Programme\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll gespeichert.

### Aktivieren der Aufzeichnung von benutzerdefinierten Ereignissen auf einem Server

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Aufzeichnung**.
4. Aktivieren Sie unter **Benutzerdefinierte Ereignisaufzeichnung** das Kontrollkästchen **Anwendungen von Drittherstellern können benutzerdefinierte Daten auf diesem XenApp-Server aufzeichnen**.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Aktivieren und Deaktivieren von Livesitzungswiedergabe und Wiedergabeschutz

Jul 08, 2016

## Aktivieren oder Deaktivieren der Wiedergabe von Livesitzungen

Mit dem Sitzungsaufzeichnungsplayer können Sie eine Sitzung nach oder während der Aufzeichnung anzeigen. Wenn Sie eine Sitzung anzeigen, die momentan aufgezeichnet wird, ähnelt es der Liveanzeige von Aktionen. Es besteht jedoch eine Verzögerung von bis zu zwei Sekunden, bis die Daten vom XenApp- bzw. XenDesktop-Server zur Arbeitsstation übermittelt werden.

Einige Funktionen stehen nicht zur Verfügung, wenn Sie Sitzungen anzeigen, deren Aufzeichnung noch nicht abgeschlossen ist:

- Eine digitale Signatur kann erst nach dem Abschluss der Aufzeichnung zugewiesen werden. Wenn die digitale Signatur aktiviert ist, können Sie Livesitzungen wiedergeben, die jedoch nicht signiert sind. Zertifikate können erst nach dem Abschluss der Aufzeichnung angezeigt werden.
- Der Wiedergabeschutz kann erst nach dem Abschluss der Aufzeichnung angewendet werden. Wenn der Wiedergabeschutz aktiviert ist, können Sie Livesitzungen wiedergeben, die jedoch erst nach dem Abschluss der Aufzeichnung verschlüsselt werden.
- Eine Datei kann erst nach dem Abschluss der Aufzeichnung zwischengespeichert werden.

In der Standardeinstellung ist die Wiedergabe von Livesitzungen aktiviert.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Wiedergabe.
4. Aktivieren Sie das Kontrollkästchen Wiedergabe von Livesitzungen zulassen oder heben Sie die Markierung auf.

## Aktivieren oder Deaktivieren des Wiedergabeschutzes

Als Sicherheitsmaßnahme werden Aufzeichnungsdateien automatisch von der Sitzungsaufzeichnung verschlüsselt, bevor sie zum Anzeigen im Sitzungsaufzeichnungsplayer heruntergeladen werden. Dieser Wiedergabeschutz stellt sicher, dass die Dateien nur von dem Benutzer, der die Datei heruntergeladen hat, und nicht von anderen Benutzern kopiert oder angezeigt werden können. Die Wiedergabe der Dateien kann nicht auf einer anderen Arbeitsstation oder von einem anderen Benutzer durchgeführt werden. Verschlüsselte Dateien haben eine ICLE-Erweiterung, nicht verschlüsselte Dateien haben eine ICL-Erweiterung. Die Dateien bleiben während der Speicherung im Cache auf der Arbeitsstation mit dem Sitzungsaufzeichnungsplayer verschlüsselt, bis sie von einem autorisierten Benutzer geöffnet werden.

Citrix empfiehlt die Verwendung von HTTPS für den Schutz der übermittelten Daten.

In der Standardeinstellung ist der Wiedergabeschutz aktiviert.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe**.
4. Aktivieren Sie das Kontrollkästchen **Für die Wiedergabe heruntergeladene Sitzungsaufzeichnungsdateien verschlüsseln** oder heben Sie die Markierung auf.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Aktivieren oder Deaktivieren der digitalen Signatur

Jul 08, 2016

Wenn Sie Zertifikate auf dem Computer installiert haben, auf dem die Komponenten der Sitzungsaufzeichnung installiert sind, können Sie die Sicherheit der Sitzungsaufzeichnungsbereitstellung erhöhen, indem Sie den Sitzungsaufzeichnungen digitale Signaturen zuweisen.

Standardmäßig ist die digitale Signierung deaktiviert. Nachdem Sie das Zertifikat zum Signieren der Aufzeichnungen ausgewählt haben, gewährt die Sitzungsaufzeichnung Leseberechtigung für den Storage Manager-Dienst der Sitzungsaufzeichnung.

## Aktivieren digitaler Signaturen

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Signatur.
4. Navigieren Sie zu dem Zertifikat, das die sichere Kommunikation zwischen den Computern ermöglicht, auf denen die Komponenten der Sitzungsaufzeichnung installiert sind.

## Deaktivieren digitaler Signaturen

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Signatur.
4. Klicken Sie auf Entfernen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Angeben des Speicherorts für Aufzeichnungen

Jul 08, 2016

In den Eigenschaften des Sitzungsaufzeichnungsservers geben Sie den Speicherort für Aufzeichnungen und archivierte Aufzeichnungen an.

Hinweis: Archivieren oder stellen Sie gelöschte Dateien mit dem Befehl icldb wieder her.

## Angeben des Speicherorts für aufgezeichnete Dateien

In der Standardeinstellung werden Aufzeichnungen im Verzeichnis Laufwerk:**\SessionRecordings** des Computers mit dem Sitzungsaufzeichnungsserver gespeichert. Sie können das Verzeichnis ändern, in dem die Aufzeichnungen gespeichert werden, weitere Verzeichnisse hinzufügen, um die Last auf mehrere Volumes zu verteilen oder freien Speicherplatz zu nutzen. Mehrere Verzeichnisse in der Liste geben an, dass die Last der Aufzeichnungen auf mehrere Verzeichnisse verteilt wird. Sie können ein Verzeichnis mehrmals hinzufügen. Der Lastausgleich durchläuft alle Verzeichnisse.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Speicherung.
4. Mit der Liste Verzeichnisse für Dateispeicherung verwalten Sie die Verzeichnisse, in denen Aufzeichnungen gespeichert werden.

Nach der Auswahl der Verzeichnisse erhalten die Dienste der Sitzungsaufzeichnung für die Verzeichnisse Vollzugriff.

Sie können die Verzeichnisse für die Dateispeicherung auf dem lokalen Datenträger, einem SAN-Volume oder an einem durch UNC-Pfad angegebenen Speicherort erstellen. Buchstaben zugeordneter Netzwerklaufwerke werden nicht unterstützt. Die Sitzungsaufzeichnung darf nicht zusammen mit NAS (Network-Attached Storage) verwendet werden, da schwere Leistungs- und Sicherheitsprobleme auftreten, die mit dem Schreiben von Aufzeichnungsdaten in ein Netzlaufwerk verbunden sind.

## Angeben eines Wiederherstellungsverzeichnisses für archivierte Dateien

In der Standardeinstellung werden Aufzeichnungen im Verzeichnis Laufwerk:**\SessionRecordingsRestore** des Computers mit dem Sitzungsaufzeichnungsserver wiederhergestellt. Sie können das Verzeichnis für die archivierten Aufzeichnungen ändern.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Speicherung.
4. Geben Sie im Feld Wiederherstellungsverzeichnis für archivierte Dateien das Verzeichnis für wieder hergestellten Archivdateien an.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Angeben der Dateigröße für Aufzeichnungen

Jul 08, 2016

Wenn die Größe der Aufzeichnungsdateien zunimmt, kann der Download kann länger dauern und die Reaktionszeit kann sich verlangsamen, wenn Sie mit dem Schieberegler durch die Wiedergabe navigieren. Sie können die Dateigröße durch Festlegen eines Schwellenwerts für eine Datei steuern. Wenn die Aufzeichnung dieses Limit erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue, um die Aufzeichnung fortzusetzen. Dies wird Rollover genannt.

**Wichtig:** Die Rollovereinstellung gilt nicht für VDI-Desktopsitzungen für XenDesktop 7.8 und den Sitzungsaufzeichnungsagent. Hier hat jede Aufzeichnungsdatei eine maximale Größe von 1 GB. Nach Erreichen dieses Limits werden Vorgänge nicht weiter aufgezeichnet.

Sie können zwei Schwellenwerte für ein Rollover angeben:

- **Dateigröße:** Wenn die Größe der Datei die angegebene Zahl Megabytes erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue. In der Standardeinstellung wird ein Dateirollover durchgeführt, wenn die Dateigröße 50 Megabytes erreicht. Sie können jedoch ein Limit von 10 Megabytes bis zu 1 Gigabyte festlegen.
- **Dauer:** Wenn die Sitzung für die angegebene Anzahl der Stunden aufgezeichnet wurde, wird die Datei geschlossen und eine neue Datei wird geöffnet. In der Standardeinstellung wird ein Dateirollover durchgeführt, wenn die Sitzung für 12 Stunden aufgezeichnet wurde. Sie können jedoch ein Limit von einer bis zu 24 Stunden festlegen.

Die Sitzungsaufzeichnung prüft beide Felder und ermittelt, welches Ereignis zuerst auftritt, und legt dann den Rollover fest. Beispiel: Wenn Sie 17 MB für die Dateigröße und sechs Stunden für die Dauer eingeben, und die Aufzeichnung erreicht 17 MB nach drei Stunden, reagiert die Sitzungsaufzeichnung auf die Dateigröße von 17 MB, schließt die Datei und öffnet eine neue.

Unabhängig vom eingegebenen Wert für die Dateigröße führt die Sitzungsaufzeichnung ein Rollover frühestens nach einer Stunde durch (dies ist der Mindestwert, den Sie eingeben können), um das Erstellen von zu vielen kleinen Dateien zu vermeiden. Diese Regel gilt nicht, wenn die Dateigröße über ein Gigabyte ansteigt.

## Angeben eines Höchstlimits für eine Datei

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsserver - Eigenschaften.
3. Klicken Sie unter Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Rollover.
4. Geben Sie ein Ganzzahl zwischen 10 und 1024 ein, mit der Sie die maximale Dateigröße in Megabyte angeben.
5. Geben Sie ein Ganzzahl zwischen 1 und 24 ein, mit der Sie die maximale Aufzeichnungslänge in Stunden angeben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anzeigen von Aufzeichnungen

Jul 08, 2016

Mit dem Sitzungsaufzeichnungsplayer zeigen Sie aufgezeichnete XenApp- bzw. XenDesktop-Sitzungen an, suchen die Sitzungsaufzeichnungsdateien und fügen Textmarken hinzu.

Wenn Sitzungen mit aktiviertem Liveplayback aufgezeichnet werden, können Sie aktuell ausgeführte Sitzungen mit einer Verzögerung von ein paar Minuten und abgeschlossene Sitzungen anzeigen.

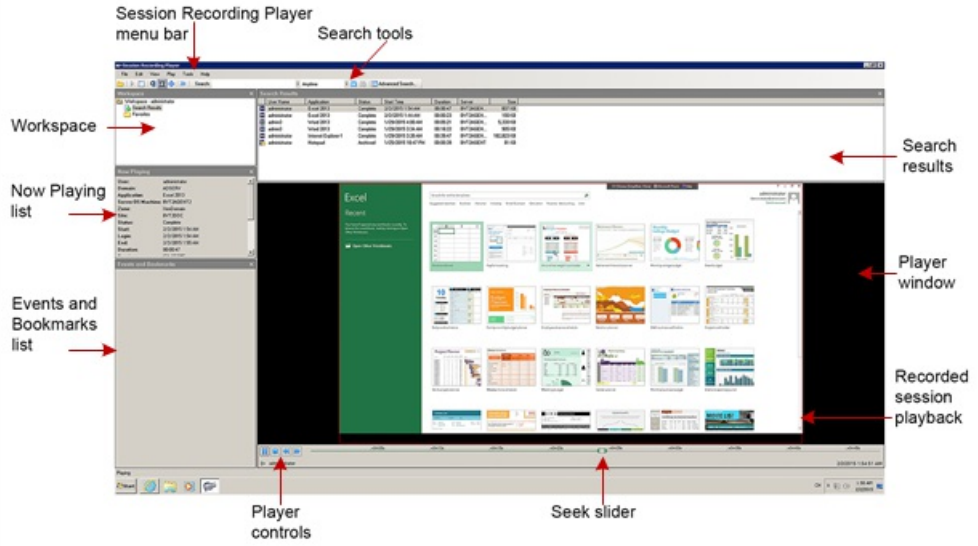
Sitzungen, die länger als die vom Sitzungsaufzeichnungsadministrator festgelegten Höchstwerte sind oder deren Dateigröße das Limit übersteigt, werden in mehreren Sitzungsdateien aufgezeichnet.

Hinweis: Der Sitzungsaufzeichnungsadministrator muss die Benutzer für den Zugriff auf aufgezeichnete Serverbetriebssystemmaschinen-Sitzungen berechtigen. Wenden Sie sich an den Sitzungsaufzeichnungsadministrator, wenn Sie nicht auf Sitzungsaufzeichnungen zugreifen können.
Bei der Installation des Sitzungsaufzeichnungsplayers richtet der Administrator normalerweise die Verbindung zwischen dem Player und einem Sitzungsaufzeichnungsserver ein. Wenn die Verbindung nicht eingerichtet ist, müssen Sie die Verbindung beim ersten Suchen nach Dateien angeben. Weitere Informationen zum Einrichten der Verbindung erhalten Sie vom Sitzungsaufzeichnungsadministrator.

## Starten des Sitzungsaufzeichnungsplayers

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
   Der Sitzungsaufzeichnungsplayer wird angezeigt.

Die Abbildung zeigt den Sitzungsaufzeichnungsplayer mit Beschriftungen seiner wichtigsten Elemente. Die Funktion dieser Elemente wird in den folgenden Artikeln beschrieben.




## Ausblenden oder Einblenden der Fensterelemente

Der Sitzungsaufzeichnungsplayer hat Fensterelemente, die Sie ein- und ausblenden können.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Ansicht.
4. Wählen Sie die Elemente aus, die Sie anzeigen möchten. Bei der Auswahl eines Elements wird es sofort angezeigt. Ein Häkchen gibt die Auswahl des Elements an.

### Wechseln des Sitzungsaufzeichnungsservers

Wenn der Administrator eine Verbindung mit mehreren Sitzungsaufzeichnungsservern im Sitzungsaufzeichnungsplayer ermöglicht hat, können Sie den Server wählen, mit dem der Player eine Verbindung herstellen soll. Der Sitzungsaufzeichnungsplayer kann nur jeweils eine Verbindung mit einem Sitzungsaufzeichnungsserver herstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Verbindungen.
4. Wählen Sie den Sitzungsaufzeichnungsserver aus, mit dem Sie eine Verbindung herstellen möchten.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Öffnen und Wiedergeben von Aufzeichnungen

Jul 08, 2016

Sie öffnen Sitzungsaufzeichnungen im Sitzungsaufzeichnungsplayer auf dreierlei Weise:

- Führen Sie eine Suche mit dem Sitzungsaufzeichnungsplayer durch. Sitzungsaufzeichnungen, die die Suchkriterien erfüllen, werden im Bereich der Suchergebnisse angezeigt.
- Greifen Sie auf Sitzungsaufzeichnungsdateien direkt von der lokalen Festplatte oder einem freigegebenen Laufwerk zu.
- Greifen Sie auf Sitzungsaufzeichnungsdateien vom Ordner "Favoriten" zu

Beim Öffnen einer Datei, die ohne digitale Signatur aufgezeichnet wurde, werden Sie in einer Warnmeldung darauf hingewiesen, dass der Ursprung und die Integrität der Datei nicht geprüft werden konnte. Bestätigen Sie die Warnmeldung mit Ja und öffnen Sie die Datei, wenn Sie hinsichtlich der Integrität der Datei keine Bedenken haben.

## Öffnen und Wiedergeben einer Aufzeichnung im Bereich der Suchergebnisse

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Führen Sie eine Suche durch.
4. Wählen Sie im Arbeitsbereich Suchergebnisse aus, wenn der Bereich "Suchergebnisse" nicht angezeigt wird.
5. Wählen Sie im Bereich der Suchergebnisse die Sitzung aus, die Sie wiedergeben möchten.
6. Tun Sie Folgendes:
   - Doppelklicken Sie auf die Sitzung.
   - Klicken Sie mit der rechten Maustaste und wählen Sie Wiedergabe.
   - Klicken Sie auf der Sitzungsaufzeichnungsplayer-Menüleiste auf Wiedergabe > Wiedergabe.

## Öffnen und Wiedergeben einer Aufzeichnung durch Zugriff auf die Datei

Namen der Sitzungsaufzeichnungsdateien beginnen mit i_, dann folgt eine eindeutige alphanumerische Datei-ID, der die Dateierweiterung .icl bzw. .icle folgt, wobei: .icl für Aufzeichnungen ohne Wiedergabeschutz und .icle für Aufzeichnungen mit Wiedergabeschutz verwendet wird. Die Sitzungsaufzeichnung speichert die Sitzungsaufzeichnungsdateien in einer Dateistruktur, in die das Datum der Aufzeichnung integriert ist. Beispiel: Die Datei für eine Sitzung, die am Montag, 22. Dezember 2014 aufgezeichnet wurde, wird im Ordnerpfad 2014\12\22 gespeichert.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Tun Sie Folgendes:
   - Wählen Sie auf der Sitzungsaufzeichnungsplayer-Menüleiste auf Datei > Öffnen aus und navigieren Sie zu der Datei.
   - Navigieren Sie mit dem Windows-Explorer auf die Datei und ziehen Sie sie in das Player-Fenster.
   - Navigieren Sie mit dem Windows-Explorer auf die Datei und doppelklicken Sie.
   - Wenn Sie Favoriten im Arbeitsbereich erstellt haben, wählen Sie Favoriten und öffnen Sie die Datei im Bereich "Favoriten" genauso wie Sie die Datei im Bereich der Suchergebnisse öffnen.

## Verwenden von Favoriten

Das Erstellen von Favoriten-Ordnern ermöglicht den schnellen Zugriff auf oft angezeigte Sitzungsaufzeichnungen. Diese Favoriten-Ordner verweisen auf Sitzungsaufzeichnungsdateien, die auf der Arbeitsstation oder auf einem Netzwerklaufwerk gespeichert sind. Sie können diese Dateien von anderen Arbeitsstationen importieren, zu anderen exportieren und die Ordner für andere Sitzungsaufzeichnungsplayer-Benutzer freigeben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Nur Benutzer mit Zugriffsrechten für den Sitzungsaufzeichnungsplayer können die Sitzungsaufzeichnungsdateien herunterladen, die den Favoriten-Ordnern zugeordnet sind. Wenden Sie sich für Zugriffsrechte an den Sitzungsaufzeichnungsadministrator.

Erstellen eines Favoriten-Unterordners

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Wählen Sie im Sitzungsaufzeichnungsplayer den Ordner Favoriten im Bereich "Arbeitsbereich".
4. Klicken Sie auf der Menüleiste auf Datei > Ordner > Neuer Ordner. Ein neuer Ordner wird unter dem Ordner Favoriten angezeigt.
5. Geben Sie den Namen des Ordners ein und drücken Sie die Eingabetaste oder klicken Sie an beliebiger Stelle, um den neuen Namen einzugeben.

Mit den anderen Optionen im Menü Datei > Ordner können Sie die Ordner löschen, umbenennen, verschieben, kopieren, importieren und exportieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Suchen nach Sitzungsaufzeichnungen

Jul 08, 2016

Im Sitzungsaufzeichnungsplayer können Sie Schnellsuchen und erweiterte Suchen durchführen und Optionen festlegen, die für alle Suchen gelten. Die Suchergebnisse werden im Bereich "Suchergebnisse" des Sitzungsaufzeichnungsplayers angezeigt.

Hinweis: Wenn Sie alle verfügbaren Sitzungsaufzeichnungen (bis zur Höchstanzahl der in einer Suche angezeigten Sitzungen) anzeigen möchten, führen Sie die Suche ohne Suchparameter durch.

## Ausführen einer Schnellsuche

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Definieren Sie die Suchkriterien:
   - Geben Sie im Feld Suchen ein Suchkriterium ein. Als Hilfestellung:
   - Zeigen Sie auf Suchen, um eine Liste der Parameter als Richtlinie zu anzuzeigen.
   - Klicken Sie auf den Pfeil rechts neben dem Feld Suchen, um den Text für die letzten 64 Suchen anzuzeigen.
   - Wählen Sie in der rechts neben dem Feld Suchen angezeigten Dropdownliste den Zeitraum oder die Dauer aus und geben Sie an, wann die Sitzung aufgezeichnet wurde.
4. Klicken Sie auf das Fernglas-Symbol rechts von der Dropdownliste, um die Suche zu starten.

## Durchführen einer erweiterten Suche

Tipp: Die erweiterte Suche kann bis zu 20 Sekunden dauern, wenn das Ergebnis über 150.000 Einheiten umfasst. Citrix empfiehlt die Verwendung gezielterer Suchbedingungen, z. B. einen Datumsbereich oder Benutzer, um den Umfang des Ergebnisses zu limitieren.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Sitzungsaufzeichnungsplayer-Fenster auf der Symbolleiste auf Erweiterte Suche oder wählen Sie Extras > Erweiterte Suche.
4. Legen Sie die Suchkriterien auf den Registerkarten im Dialogfeld Erweiterte Suche fest:
   - Allgemein ermöglicht die Suche nach Domäne oder Kontoautorität, Site, Gruppe, Serverbetriebssystemmaschine, Anwendung oder Datei-ID.
   - Datum/Uhrzeit: Die Suche wird nach Datum, Wochentag und Tageszeit durchgeführt.
   - Ereignisse dient zur Suche nach benutzerdefinierten Ereignissen, die der Sitzungsaufzeichnungsadministrator in die Sitzungen eingefügt hat.
   - Sonstiges: Die Suche wird nach Sitzungsname, Clientname, Clientadresse und Aufzeichnungsdauer durchgeführt. Sie können für diese Suche auch die Höchstzahl der angezeigten Suchergebnisse und den Einschluss von archivierten Dateien in der Suche festlegen.

   Bei der Angabe von Suchkriterien wird die Abfrage, die Sie erstellen, im unteren Bereich des Dialogfelds angezeigt.
5. Klicken Sie auf Suchen, um die Suche zu starten.

Tipp: Sie können erweiterte Suchen speichern und abrufen. Klicken Sie im Dialogfeld Erweiterte Suche auf Speichern, um die aktuelle Abfrage zu speichern. Klicken Sie im Dialogfeld Erweiterte Suche auf Öffnen, um eine gespeicherte Abfrage abzurufen. Abfragen werden als Dateien mit der ISQ-Erweiterung gespeichert.

## Einstellen von Suchoptionen

Mit den Suchoptionen im Sitzungsaufzeichnungsplayer beschränken Sie die Höchstzahl der Sitzungsaufzeichnungen, die in


© 1999-2017 Citrix Systems, Inc. All rights reserved.

den Suchergebnissen angezeigt werden, und legen den Ein- oder Ausschluss von archivierten Sitzungsaufzeichnungsdateien fest.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Suche.
4. Geben Sie im Feld Angezeigte Ergebnisse (max.) die Anzahl der Suchergebnisse ein, die angezeigt werden. Sie können maximal 500 Ergebnisse anzeigen.
5. Abhängig davon, ob Sie archivierte Dateien in Suchen einschließen möchten, aktivieren oder deaktivieren Sie Archivierte Dateien einschließen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Wiedergeben aufgezeichneter Sitzungen

Jul 08, 2016

Nach dem Öffnen einer aufgezeichneten Sitzung im Sitzungsaufzeichnungsplayer können Sie in der Aufzeichnung folgendermaßen navigieren:

- Mit den Player-Bedienelementen können Sie die Aufzeichnung wiedergeben, anhalten oder stoppen und die Wiedergabegeschwindigkeit erhöhen oder verringern.
- Mit dem Schieberegler für das Positionieren gehen Sie vorwärts oder rückwärts.

Wenn Sie Marker in die Aufzeichnung eingefügt haben, oder die aufgezeichnete Sitzung benutzerdefinierte Ereignisse enthält, können Sie mit diesen Markern oder Ereignissen durch die Sitzungsaufzeichnung navigieren.

Hinweis:

- Bei der Wiedergabe einer aufgezeichneten Sitzung wird möglicherweise ein zweiter Mauszeiger angezeigt. Der zweite Mauszeiger wird an der Stelle in der Aufzeichnung angezeigt, an der der Benutzer in Internet Explorer navigiert und auf ein Bild geklickt hat, das im Original größer als der Bildschirm war, das jedoch von Internet Explorer automatisch skaliert wurde. Ein Zeiger wird während der Sitzung angezeigt, jedoch können zwei bei der Wiedergabe angezeigt werden.
- Diese Version der Sitzungsaufzeichnung unterstützt weder die SpeedScreen-Multimediabeschleunigung für XenApp noch die Richtlinieneinstellung zum Optimieren der Flash-Inhalte für XenApp. Wenn diese Option aktiviert ist, wird bei der Wiedergabe ein schwarzes Rechteck angezeigt.
- Die Sitzungsaufzeichnung kann keine Lync-Webcamvideos aufzeichnen, wenn das HDX RealTime Optimization Pack verwendet wird.

## Verwenden der Player-Bedienelemente

Sie können auf die Player-Bedienelemente unten im Player-Fenster klicken oder im Sitzungsaufzeichnungsplayer-Menü auf Wiedergabe klicken. Die Player-Bedienelemente ermöglichen Folgendes:

| | |
|---|---|
| | Wiedergeben der ausgewählten Sitzungsdatei. |
| | Anhalten der Wiedergabe. |
| | Stoppen der Wiedergabe. Wenn Sie auf Stopp und dann auf Wiedergabe klicken, wird die Aufzeichnung vom Anfang der Datei an wiedergegeben. |
| | Halbieren der momentanen Wiedergabegeschwindigkeit um die Hälfte auf mindestens ein Viertel der Normalgeschwindigkeit. |
| | Verdoppeln der momentanen Wiedergabegeschwindigkeit auf maximal das Zweiunddreißigfache der Normalgeschwindigkeit. |

## Verwenden des Schiebereglers für das Positionieren

Mit dem Schieberegler für das Positionieren unter dem Player-Fenster springen Sie auf eine andere Stelle in der aufgezeichneten Sitzung. Sie können den Schieberegler für das Positionieren auf eine Stelle in der Aufzeichnung ziehen, die Sie anzeigen möchten, oder auf eine Stelle auf dem Schieberegler klicken, um auf diese Stelle zu gehen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sie können den Schieberegler für das Positionieren auch mit den folgenden Tasten auf der Tastatur steuern:

| Schlüssel: | Positionieren: |
|---|---|
| Pos1 | Auf den Anfang positionieren |
| Ende | Auf das Ende positionieren |
| Nach-Rechts-Taste | 5 Sekunden vorwärts positionieren |
| Nach-Links-Taste | 5 Sekunden rückwärts positionieren |
| Verschieben des Mausrads um einen Anschlag nach unten | 15 Sekunden vorwärts positionieren |
| Verschieben des Mausrads um einen Anschlag nach oben | 15 Sekunden rückwärts positionieren |
| Strg + Nach-Rechts-Taste | 30 Sekunden vorwärts positionieren |
| Strg + Nach-Links-Taste | 30 Sekunden rückwärts positionieren |
| Bild-Ab | 1 Minute vorwärts positionieren |
| Bild-Auf | 1 Minute rückwärts positionieren |
| Strg + Mausrad einen Klick nach unten bewegen | 90 Sekunden vorwärts positionieren |
| Strg + Mausrad einen Klick nach oben bewegen | 90 Sekunden rückwärts positionieren |
| Strg + Bild-Ab | 6 Minuten vorwärts positionieren |
| Strg + Bild-Auf | 6 Minuten rückwärts positionieren |

Hinweis: Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Player und verschieben Sie den Schieberegler, um die Reaktionszeit des Schiebereglers zu verlängern oder zu verkürzen. Für eine schnellere Reaktionszeit wird mehr Speicher benötigt. Die Reaktion kann, abhängig von der Größe der Aufzeichnungen und der Computerhardware, langsam sein.

## Ändern der Wiedergabegeschwindigkeit

Sie können die Wiedergabe aufgezeichneter Sitzungen im Sitzungsaufzeichnungsplayer in exponentiellen Erhöhungen von einem Viertel der normalen Wiedergabegeschwindigkeit bis zum 32-fachen der normalen Wiedergabegeschwindigkeit


© 1999-2017 Citrix Systems, Inc. All rights reserved.

einstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Sitzungsaufzeichnungsplayer-Menüleiste auf Wiedergabe > Wiedergabegeschwindigkeit.
4. Wählen Sie eine der Optionen für die Geschwindigkeit aus.

Die Geschwindigkeit wird sofort geändert. Eine Zahl gibt die erhöhte oder verringerte Wiedergabegeschwindigkeit unter den Bedienelementen im Player-Fenster an. Text, der die exponentielle Rate angibt, wird kurz in grün im Player-Fenster angezeigt.

### Überspringen von Stellen ohne Aktionen

Im Schnellprüfmodus überspringt der Sitzungsaufzeichnungsplayer die Teile von aufgezeichneten Sitzungen, in denen keine Aktion stattfindet. Mit dieser Einstellung sparen Sie Zeit bei der Wiedergabe, animierte Folgen werden jedoch nicht übersprungen, z. B. ein animierter Mauszeiger, blinkende Cursor oder angezeigte Uhren, bei denen sich die zweite Hand bewegt.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Wiedergabe > Schnellprüfmodus.

Sie können die Option aktivieren oder deaktivieren. Bei jeder Auswahl wird der Status kurz in grün im Player -Fenster angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verwenden von Ereignissen und Textmarken

Jul 08, 2016

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen.

Ereignisse werden bei der Aufzeichnung mit der Ereignis-API oder einer Anwendung eines Drittherstellers in die Sitzungen eingefügt. Ereignisse werden als Teil der Sitzungsdatei gespeichert. Sie können mit dem Sitzungsaufzeichnungsplayer nicht gelöscht oder geändert werden.

Textmarken sind Marker, die Sie mit dem Sitzungsaufzeichnungsplayer in Sitzungsaufzeichnungen einfügen. Textmarken werden der aufgezeichneten Sitzung zugeordnet, bis sie gelöscht werden, sie werden jedoch nicht mit der Sitzungsdatei gespeichert. In der Standardeinstellung ist jede Textmarke mit Textmarke beschriftet. Sie können diese Beschriftung beliebig ändern und maximal 128 Zeichen eingeben.

Ereignisse und Textmarken werden als Punkte unter dem Player-Fenster angezeigt. Ereignisse werden als gelbe Punkte und Textmarken als blaue Punkte angezeigt. Wenn Sie die Maus auf diese Punkte verschieben, wird der zugeordnete Text angezeigt. Sie können die Ereignisse und Textmarken auch in der Liste "Ereignisse und Textmarken" im Sitzungsaufzeichnungsplayer anzeigen. Sie werden in dieser Liste in chronologischer Reihenfolge mit den Textbeschriftungen und den Uhrzeiten angezeigt, zu denen sie in der aufgezeichneten Sitzung erscheinen.

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen. Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springen Sie auf die Stelle in der aufgezeichneten Sitzung, an der das Ereignis oder die Textmarke eingefügt ist.

## Anzeigen von Ereignissen und Textmarken in der Liste

In der Liste "Ereignisse und Textmarken" werden die Ereignisse und Textmarken angezeigt, die in der momentan wiedergegebenen Sitzungsaufzeichnung eingefügt sind. Sie können in der Liste nur Ereignisse, nur Textmarken oder Ereignisse und Textmarken anzeigen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Verschieben Sie den Mauszeiger auf die Liste "Ereignisse und Textmarken" und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
4. Wählen Sie Nur Ereignisse anzeigen, Nur Textmarken anzeigen oder Alle anzeigen.

## Einfügen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Starten Sie die Wiedergabe der aufgezeichneten Sitzung, der Sie eine Textmarke hinzufügen möchten.
4. Schieben Sie den Schieberegler für das Positionieren auf die Stelle, an der Sie die Textmarke einfügen möchten.
5. Schieben Sie den Mauszeiger in den Player-Fensterbereich und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Fügen Sie eine Textmarke mit der Standardbeschriftung Textmarke hinzu oder erstellen Sie eine Anmerkung:
   - Zum Hinzufügen einer Textmarke mit der Standardbeschriftung Textmarke wählen Sie Textmarke hinzufügen.
   - Zum Hinzufügen einer Textmarke mit einer eigenen Beschriftung wählen Sie Anmerkung hinzufügen. Geben Sie die Anmerkung (max. 128 Zeichen) ein, die Sie der Textmarke zuordnen möchten. Klicken Sie auf OK.

## Hinzufügen oder Ändern einer Anmerkung


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nach dem Erstellen einer Textmarke können Sie eine Anmerkung hinzufügen oder eine bestehende Anmerkung ändern.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Starten Sie die Wiedergabe der aufgezeichneten Sitzung, die die Textmarke enthält.
4. Stellen Sie sicher, dass Textmarken in der Liste "Ereignisse und Textmarken" angezeigt werden.
5. Wählen Sie die Textmarke aus der Liste "Ereignisse und Textmarken" aus und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Wählen Sie Anmerkung bearbeiten.
7. Geben Sie im angezeigten Dialogfeld die neue Anmerkung ein und klicken Sie auf OK.

### Löschen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Starten Sie die Wiedergabe der aufgezeichneten Sitzung, die die Textmarke enthält.
4. Stellen Sie sicher, dass Textmarken in der Liste "Ereignisse und Textmarken" angezeigt werden.
5. Wählen Sie die Textmarke aus der Liste "Ereignisse und Textmarken" aus und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Wählen Sie Löschen.

### Gehen auf ein Ereignis oder eine Textmarke

Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springt der Sitzungsaufzeichnungsplayer an die Stelle in der Sitzungsaufzeichnung, an der das Ereignis oder die Textmarke eingefügt ist.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Starten Sie eine Sitzungsaufzeichnung, die Ereignisse oder Textmarken enthält.
4. Gehen Sie auf ein Ereignis oder eine Textmarke.
   - Klicken Sie im Bereich unter dem Player-Fenster auf den Punkt, der das Ereignis oder die Textmarke darstellt, um auf das Ereignis oder die Textmarke zu gehen.
   - Doppelklicken Sie in der Liste "Ereignisse und Textmarken" auf ein Ereignis oder eine Textmarke, um an die entsprechende Stelle zu gehen. Wenn Sie auf das nächste Ereignis oder die nächste Textmarke gehen möchten, wählen Sie ein Ereignis oder eine Textmarke aus der Liste aus, klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen, und wählen Sie Auf Textmarke positionieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Ändern der Wiedergabeanzeige

Jul 08, 2016

Mit Optionen können Sie ändern, wie die aufgezeichneten Sitzungen im Player-Fenster angezeigt werden. Sie können das Bild mit Panning und Skalieren ändern, die Wiedergabe im Vollbildmodus anzeigen, das Player-Fenster in einem eigenen Fenster und einen Rahmen um die Sitzungsaufzeichnung anzeigen, um sie vom Hintergrund des Player-Fensters zu unterscheiden.

## Anzeigen des Player-Fensters im Vollbildmodus

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Ansicht > Player-Vollbild.
4. Drücken Sie ESC oder F11, um die Originalgröße des Fensters wiederherzustellen.

## Anzeigen des Player-Fensters in einem eigenen Fenster

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Ansicht > Player in neuem Fenster. Ein neues Fenster wird mit dem Player-Fenster angezeigt. Sie können das Fenster verschieben oder die Fenstergröße ändern.
4. Wenn Sie das Player-Fenster im Hauptfenster einbetten möchten, wählen Sie Ansicht > Player in neuem Fenster oder drücken Sie F10.

## Skalieren der Sitzungswiedergabe auf die Größe des Player-Fensters

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Wiedergabe > Panning und Skalieren > Passend skalieren.
   - Bei Passend skalieren (Schnellrendering) wird das Bild verkleinert, die Bildqualität ist jedoch noch gut. Bilder werden schneller als mit der Option "Passend skalieren (hohe Qualität)" aufgebaut, die Bilder und der Text sind jedoch nicht so scharf. Verwenden Sie diese Option, wenn Sie Leistungsprobleme mit der Option "Passend skalieren (hohe Qualität)" feststellen.
   - Bei Passend skalieren (hohe Qualität) wird das Bild verkleinert, die Qualität des Bildes und des Textes ist sehr gut. Bei dieser Option werden die Bilder möglicherweise langsamer als bei der Option "Passend skalieren (Schnellrendering)" aufgebaut.

## Durchführen von Panning des Bilds

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie im Menü des Sitzungsaufzeichnungsplayers auf Wiedergabe > Panning und Skalieren > Panning. Der Zeiger ändert sich zu einer Hand und eine kleine Darstellung des Bildschirms wird oben rechts im Player-Fenster angezeigt.
4. Ziehen Sie das Bild. Die kleine Darstellung gibt die Stelle im Bild an, an der Sie sich befinden.
5. Wählen Sie eine der Skalierungsoptionen, um das Panning anzuhalten.

## Anzeigen eines roten Rahmens um die Sitzungsaufzeichnung

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Player.
4. Aktivieren Sie Rahmen um Sitzungsaufzeichnung anzeigen.
   Tipp: Ist Rahmen um Sitzungsaufzeichnung anzeigen nicht aktiviert, können Sie den roten Rahmen vorübergehend anzeigen, indem Sie die linke Maustaste gedrückt halten, wenn der Zeiger im Player-Fenster ist.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Zwischenspeichern von Sitzungsaufzeichnungsdateien

Jul 08, 2016

Bei jedem Öffnen einer Sitzungsaufzeichnungsdatei lädt der Sitzungsaufzeichnungsplayer die Datei vom Speicherort herunter, auf dem die Aufzeichnungen gespeichert sind. Wenn Sie dieselben Dateien oft herunterladen, sparen Sie Zeit, wenn Sie die Dateien auf der Arbeitsstation zwischenspeichern. Zwischengespeicherte Dateien werden auf der Arbeitsstation in diesem Ordner gespeichert:

userprofile\AppData\Local\Citrix\SessionRecording\Player\Cache

Sie können die verwendete Cachegröße angeben. Wenn die Aufzeichnungen den angegebenen Speicherplatz auf der Festplatte vollständig belegen, löscht die Sitzungsaufzeichnung die ältesten und am wenigsten verwendeten Aufzeichnungen, um Platz für neue Aufzeichnungen zu machen. Sie können den Cache jederzeit leeren, um freien Speicherplatz auf der Festplatte zu erhalten.

## Aktivieren des Zwischenspeichern

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Cache.
4. Aktivieren Sie das Kontrollkästchen Heruntergeladene Dateien lokal zwischenspeichern.
5. Wenn Sie den für die Zwischenspeicherung verwendeten Speicherplatz auf dem Datenträger beschränken möchten, aktivieren Sie das Kontrollkästchen Verwendeten Speicherplatz auf Datenträger beschränken, und geben Sie den Speicherplatz in Megabyte an.
6. Klicken Sie auf OK.

## Löschen des Cache

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Cache.
4. Aktivieren Sie das Kontrollkästchen Heruntergeladene Dateien lokal zwischenspeichern.
5. Klicken Sie im Sitzungsaufzeichnungsplayer auf Extras > Optionen > Cache.
6. Klicken Sie auf Cache löschen und dann zur Bestätigung auf OK.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Problembehandlung bei der Sitzungsaufzeichnung

Jul 08, 2016

In diesen Informationen finden Sie Lösungen zu Problemen, auf die Sie möglicherweise während oder nach der Installation der Sitzungsaufzeichnungskomponenten stoßen:

- Probleme bei der Komponentenverbindung
- Probleme bei der Sitzungsaufzeichnung
- Probleme beim Sitzungsaufzeichnungsplayer oder der Richtlinienkonsole für die Sitzungsaufzeichnung
- Probleme beim Kommunikationsprotokoll

## Sitzungsaufzeichnungsagent kann keine Verbindung herstellen

Wenn der Sitzungsaufzeichnungsagent keine Verbindung herstellen kann, wird die Ereignismeldung Exception caught while sending poll messages to Session Recording Broker gefolgt vom Ausnahmetext protokolliert. Der Ausnahmetext gibt den Grund für den Verbindungsfehler an. Diese Gründe sind wie folgt:

- Die zugrunde liegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden. Diese Ausnahme bedeutet, dass der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer Zertifizierungsstelle signiert ist, die der Server mit dem Sitzungsaufzeichnungsagent nicht als vertrauenswürdig einstuft oder für die der Server kein Zertifikat der Zertifizierungsstelle hat. Das Zertifikat kann auch abgelaufen oder widerrufen sein.

  Lösung: Stellen Sie sicher, dass das richtige Zertifikat der Zertifizierungsstelle auf dem Server mit dem Sitzungsaufzeichnungsagent installiert ist oder ein vertrauenswürdiges Zertifikat verwendet wird.

- Der Remoteserver gaben einen Fehler zurück: (403) verboten. Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres Protokoll) versuchen. Der Computer mit dem Sitzungsaufzeichnungsserver lehnt die Verbindung ab, da er nur sichere Verbindungen annimmt.

  Lösung: Ändern Sie in den Eigenschaften des Sitzungsaufzeichnungsagents das Protokoll des Sitzungsaufzeichnungsbrokers in HTTPS.

Der Sitzungsaufzeichnungsbroker gab beim Auswerten einer Aufzeichnungsrichtlinienabfrage einen unbekannten Fehler zurück. Fehlercode 5 (Zugriff verweigert). Weitere Informationen finden Sie im Ereignisprotokoll auf dem Sitzungsaufzeichnungsserver. Dieser Fehler tritt auf, wenn Sitzungen gestartet werden und eine Anfrage für eine Auswertung der Aufzeichnungsrichtlinie gemacht wird. Der Fehler tritt auf, wenn die Gruppe der authentifizierten Benutzer (die Standardmitglieder) von der Rolle "PolicyQuery" in der Sitzungsaufzeichnungsautorisierungskonsole entfernt werden.

Lösung: Fügen Sie die Gruppe der authentifizierten Benutzer wieder der Rolle hinzu oder fügen Sie alle Server mit dem Sitzungsaufzeichnungsagent der Rolle "PolicyQuery" hinzu.

Die zugrunde liegende Verbindung wurde geschlossen. Eine Verbindung, die aktiv bleiben sollte, wurde vom Server geschlossen. Dieser Fehler bedeutet, dass der Sitzungsaufzeichnungsserver nicht ausgeführt wird oder keine Anfragen annehmen kann. IIS können offline geschaltet sein oder werden neu gestartet, oder der Server ist offline geschaltet.

Lösung: Stellen Sie sicher, dass der Sitzungsaufzeichnungsserver gestartet wurde, IIS auf dem Server ausgeführt wird und der Server eine Verbindung zum Netzwerk hat.

## Installation von Sitzungsaufzeichnungsserverkomponenten schlägt fehl


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Die Installation der Sitzungsaufzeichnungsserverkomponenten schlägt mit den Fehlercodes 2503 und 2502 fehl.
Lösung:
Überprüfen Sie die Zugriffssteuerungsliste (ACL) im Ordner C:\windows\Temp, um sicherzustellen, dass lokale Benutzer und Gruppen Schreibberechtigung für diesen Ordner haben. Falls nicht, fügen Sie die Schreibberechtigung manuell hinzu.

### Sitzungsaufzeichnungsplayer kann keine Verbindung mit der Datenbank für die Sitzungsaufzeichnung herstellen

Wenn der Sitzungsaufzeichnungsserver keine Verbindung mit der Datenbank für die Sitzungsaufzeichnung herstellen kann, wird möglicherweise eine Fehlermeldung mit ungefähr dem folgenden Wortlaut angezeigt:

Ereignisquelle:

**Ein netzwerkbezogener oder instanzenspezifischer Fehler trat auf, während eine Verbindung zu SQL Server hergestellt wurde**. Dieser Fehler wird mit der ID 2047 im Anwendungsereignisprotokoll der Ereignisanzeige des Computers aufgezeichnet, auf dem der Sitzungsaufzeichnungsserver gehostet wird.

Citrix Speichermanager der Sitzungsaufzeichnung - Beschreibung: Citrix: Ausnahme beim Herstellen der Datenbankverbindung. Dieser Fehler wird im Ereignisprotokoll der Anwendungen in der Ereignisanzeige des Computers mit dem Sitzungsaufzeichnungsserver aufgezeichnet.

Verbindung mit dem Sitzungsaufzeichnungsserver kann nicht hergestellt werden. Überprüfen Sie, ob der Sitzungsaufzeichnungsserver ausgeführt wird. Diese Fehlermeldung wird beim Start der Richtlinienkonsole für die Sitzungsaufzeichnung angezeigt.

Lösung:

- Die Express Edition von Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 oder Microsoft SQL Server 2014 ist auf einem eigenständigen Server installiert und Dienste oder Einstellungen sind nicht richtig für die Sitzungsaufzeichnung konfiguriert. Auf dem Server muss das TCP/IP-Protokoll aktiviert sein, und der SQL Server Browser-Dienst muss ausgeführt werden. Weitere Informationen zur Aktivierung dieser Einstellungen finden Sie in der Microsoft Dokumentation.
- Bei der Installation der Sitzungsaufzeichnung (Verwaltungskomponenten) wurden falsche Server- und Datenbankinformationen angegeben. Deinstallieren Sie die Datenbank für die Sitzungsaufzeichnung und installieren Sie sie mit den richtigen Informationen neu.
- Der Server mit der Datenbank für die Sitzungsaufzeichnung ist ausgefallen. Prüfen Sie die Serverkonnektivität.
- Der Computer mit dem Sitzungsaufzeichnungsserver oder der Computer mit dem Server für die Datenbank für die Sitzungsaufzeichnung kann den vollqualifizierten Domänennamen oder den NetBIOS-Namen des jeweils anderen nicht auflösen. Stellen Sie mit "Ping" sicher, dass die Namen aufgelöst werden können.
- Prüfen Sie, ob in der Firewallkonfiguration für die Datenbank für die Sitzungsaufzeichnung SQL Server-Verbindungen zugelassen sind. Weitere Informationen finden Sie in dem Microsoft-Artikel unter https://msdn.microsoft.com/en-us/library/cc646023.aspx.

Fehler bei der Anmeldung für Benutzer "NT_AUTHORITY\ANONYMOUS LOGON". Diese Fehlermeldung gibt an, dass die Dienste falsch als .\administrator angemeldet sind.

Lösung: Starten Sie die Dienste als lokaler Systembenutzer und die SQL-Dienste neu.

### Kein Aufzeichnen von Sitzungen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Wenn die Anwendungssitzungen nicht aufgezeichnet werden, prüfen Sie zuerst das Anwendungsereignisprotokoll in der Ereignisanzeige auf der Serverbetriebssystemmaschine, auf der der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver ausgeführt werden. Sie können nützliche Diagnoseinformationen erhalten.

Wenn Sitzungen nicht aufgezeichnet werden, kann dies folgende Gründe haben:

- **Komponentenverbindungen und Zertifikate**: Wenn die Sitzungsaufzeichnungskomponenten nicht miteinander kommunizieren können, können Sitzungsaufzeichnungen fehlschlagen. Zur Behebung von Aufzeichnungsproblemen sollten Sie sicherstellen, dass alle Komponenten richtig konfiguriert sind und auf die richtigen Computer verweisen, und dass alle Zertifikate gültig und richtig installiert sind.
- **Umgebungen ohne Active Directory-Domäne**: Die Sitzungsaufzeichnung ist für eine Ausführung in einer Microsoft Active Directory-Domänenumgebung konzipiert. Wenn Sie keine Active Directory-Umgebung ausführen, können Aufzeichnungsprobleme auftreten. Stellen Sie sicher, dass alle Komponenten der Sitzungsaufzeichnung auf Computern ausgeführt werden, die Mitglieder einer Active Directory-Domäne sind.
- **Die Sitzungsfreigabe verursacht einen Konflikt mit der aktiven Richtlinie:** Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Anwendungen, die später in derselben Sitzung geöffnet werden, halten die Richtlinie ein, die für die erste Anwendung gilt. Veröffentlichten Sie die problematischen Anwendungen auf eigenständigen Serverbetriebssystemmaschinen oder deaktivieren Sie die Sitzungsfreigabe, um einen Konflikt zwischen der Sitzungsfreigabe und der aktiven Richtlinie zu vermeiden.
- **Die Aufzeichnung ist nicht aktiviert:** Wenn Sie den Sitzungsaufzeichnungsagent auf einer Serverbetriebssystemmaschine installieren, wird die Aufzeichnung auf dem Server standardmäßig aktiviert. Die Aufzeichnung erfolgt erst, wenn eine aktive Aufzeichnungsrichtlinie konfiguriert ist, die Aufzeichnungen zulässt.
- **Die aktive Aufzeichnungsrichtlinie lässt die Aufzeichnung nicht zu.** Zum Aufzeichnen einer Sitzung muss die aktive Aufzeichnungsrichtlinie zulassen, dass die Sitzungen für den Benutzer, Server oder die veröffentlichte Anwendung aufgezeichnet werden können.
- **Die Dienste der Sitzungsaufzeichnung werden nicht ausgeführt.** Zum Aufzeichnen von Sitzungen muss der Sitzungsaufzeichnungsagent-Dienst auf der Serverbetriebssystemmaschine und der Dienst des Speichermanagers der Sitzungsaufzeichnung auf dem Computer mit dem Sitzungsaufzeichnungsserver ausgeführt werden.
- **MSMQ ist nicht konfiguriert:** Wenn MSMQ auf dem Computer mit dem Sitzungsaufzeichnungsagent und dem Computer mit dem Sitzungsaufzeichnungsserver falsch konfiguriert ist, können Aufzeichnungsprobleme auftreten.

### Wiedergabe von Livesitzungen nicht möglich

Wenn Sie Probleme beim Wiedergeben von Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

Fehler beim Download der Sitzungsaufzeichnungsdatei. Wiedergabe einer Livesitzung ist nicht zulässig. Die Konfiguration des Servers lässt diese Funktion nicht zu. Dieser Fehler gibt an, dass der Server die Aktion nicht zulässt.

Lösung: Klicken Sie in den Sitzungsaufzeichnungsserver - Eigenschaften auf die Registerkarte Wiedergabe und aktivieren Sie das Kontrollkästchen Wiedergabe von Livesitzungen zulassen.

### Aufzeichnungen sind beschädigt oder unvollständig

Wenn Aufzeichnungen beim Anzeigen im Sitzungsaufzeichnungsplayer beschädigt oder unvollständig sind, werden u. U. auch Warnungen in den Ereignisprotokollen auf dem Sitzungsaufzeichnungsagent protokolliert.

**Event Source:** Citrix Session Recording Storage Manager

**Description:** Data lost while recording file


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dies passiert normalerweise, wenn mit Maschinenerstellungsdienste (MCS) oder Provisioning Services VDAs mit einem konfigurierten Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt werden. In diesem Fall haben die VDAs die gleiche QMId für MSMQ.

Lösung: Erstellen Sie eine eindeutige QMId für jeden VDA. Einen Workaround finden Sie unter Bekannte Probleme.

### Test der Verbindung mit Datenbankinstanz schlägt bei Installation der Datenbank für Sitzungsaufzeichnung oder Sitzungsaufzeichnungsserver fehl

Bei der Installation der Datenbank für die Sitzungsaufzeichnung oder des Sitzungsaufzeichnungsservers schlägt der Test der Verbindung fehl und es wird eine **Fehlermeldung mit der Aufforderung zur Korrektur des Namens der Datenbankinstanz** angezeigt, selbst wenn dieser richtig ist.

Lösung: Stellen Sie sicher, dass der aktuelle Benutzer die öffentliche SQL Server-Rollenberechtigung hat, damit der Test nicht aufgrund einer fehlenden Berechtigung fehlschlägt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Prüfen der Komponentenverbindungen

Jul 08, 2016

Beim Setup der Sitzungsaufzeichnung stellen die Komponenten möglicherweise keine Verbindung mit den anderen Komponenten her. Alle Komponenten kommunizieren mit dem Sitzungsaufzeichnungsserver (Broker). In der Standardeinstellung ist der Broker (eine IIS-Komponente) mit dem Standardwebsitezertifikat von IIS gesichert. Wenn eine Komponente keine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen kann, kann der Verbindungsversuch der anderen Komponenten auch fehlschlagen.

Der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver (Speichermanager und Broker) protokollieren Verbindungsfehler im Ereignisprotokoll der Anwendungen in der Ereignisanzeige auf dem Computer mit dem Sitzungsaufzeichnungsserver. Die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer zeigen Fehlermeldungen auf dem Bildschirm an, wenn keine Verbindung hergestellt werden kann.

## Prüfen, ob der Sitzungsaufzeichnungsagent verbunden ist

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsagent - Eigenschaften.
3. Klicken Sie in den Sitzungsaufzeichnungsserver - Eigenschaften auf Verbindung.
4. Stellen Sie sicher, dass der Wert für Sitzungsaufzeichnungsserver den Namen des Computers enthält, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
5. Stellen Sie sicher, dass der unter Sitzungsaufzeichnungsserver angegebene Server von der Serverbetriebssystemmaschine kontaktiert werden kann.

Hinweis: Prüfen Sie das Anwendungsereignisprotokoll auf Fehler und Warnungen.

## Prüfen, ob der Sitzungsaufzeichnungsserver verbunden ist

Achtung: Die Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie den Registrierungs-Editor.
3. Navigieren Sie auf HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Stellen Sie sicher, dass der Wert für SmAudDatabaseInstance richtig auf die Datenbank für die Sitzungsaufzeichnung verweist, die Sie in der SQL Server-Instanz installiert haben.

## Prüfen, ob die Datenbank für die Sitzungsaufzeichnung verbunden ist

1. Öffnen Sie die SQL-Instanz, die die installierte Datenbank für die Sitzungsaufzeichnung enthält, in einem SQL-Verwaltungstool.
2. Öffnen Sie die Sicherheitsberechtigungen der Datenbank für die Sitzungsaufzeichnung.
3. Stellen Sie sicher, dass das Computerkonto der Sitzungsaufzeichnung Zugriffsrechte auf die Datenbank hat. Beispiel: Wenn der Server mit dem Sitzungsaufzeichnungsserver **SsRecSrv** in der MIS-Domäne genannt wird, muss das Computerkonto in der Datenbank als MIS\SsRecSrv$ konfiguriert werden. Dieser Wert wird während der Installation der Datenbank für die Sitzungsaufzeichnung konfiguriert.

## Testen der IIS-Konnektivität


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mit dem Testen der Verbindungen zwischen Sitzungsaufzeichnungsserver und IIS-Site unter Zugriff auf die Webseite des Sitzungsaufzeichnungsbrokers mit einem Webbrowser können Sie feststellen, ob Kommunikationsprobleme zwischen den Sitzungsaufzeichnungskomponenten auf eine falsche Protokollkonfiguration, Zertifizierungsprobleme oder Probleme beim Start des Sitzungsaufzeichnungsbrokers zurückzuführen sind.

## Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsagent

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
   - HTTPS: **https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: **http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Wenn ein XML-Dokument im Browser angezeigt wird, bestätigt dies, dass der Computer, auf dem der Sitzungsaufzeichnungsagent ausgeführt wird, mit dem Sitzungsaufzeichnungsserver-Computer verbunden ist und das konfigurierte Protokoll verwendet.

## Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsplayer

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
   - HTTPS: **https://servername/SessionRecordingBroker/Player.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: **http://servername/SessionRecordingBroker/Player.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Wenn ein XML-Dokument im Browser angezeigt wird, bestätigt dies, dass der Computer, auf dem der Sitzungsaufzeichnungsplayer ausgeführt wird, mit dem Sitzungsaufzeichnungsserver-Computer verbunden ist und das konfigurierte Protokoll verwendet.

## Prüfen der IIS-Konnektivität für die Richtlinienkonsole für die Sitzungsaufzeichnung

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
   - HTTPS: **https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: **http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Wenn ein XML-Dokument im Browser angezeigt wird, bestätigt dies, dass der Computer, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt wird, mit dem Sitzungsaufzeichnungsserver-Computer verbunden ist und das konfigurierte Protokoll verwendet.

### Problembehandlung bei Zertifikaten

Wenn Sie HTTPS als Kommunikationsprotokoll verwenden, muss der Computer mit dem Sitzungsaufzeichnungsserver mit


© 1999-2017 Citrix Systems, Inc. All rights reserved.

einem Serverzertifikat konfiguriert werden. Alle Komponentenverbindungen mit dem Sitzungsaufzeichnungsserver müssen ein Zertifikat der Stammzertifizierungsstelle haben. Sonst schlagen die Verbindungen zwischen den Komponenten fehl.

Sie können die Zertifikate genauso wie beim Testen der IIS-Konnektivität durch Zugriff auf die Webseite des Sitzungsaufzeichnungsbrokers testen. Wenn Sie auf die XML-Seite für jede Komponente zugreifen können, sind die Zertifikate richtig konfiguriert.

Im Anschluss finden Sie Gründe, warum Zertifikate zu Verbindungsproblemen führen:

- **Ungültige oder fehlende Zertifikate:** Wenn der Server mit dem Sitzungsaufzeichnungsagent kein Stammzertifikat für die Vertrauenswürdigkeit des Serverzertifikats hat, den Sitzungsaufzeichnungsserver nicht als vertrauenswürdig ansieht und keine Verbindung über HTTPS herstellen kann, schlägt die Verbindung fehl. Stellen Sie sicher, dass alle Komponenten das Serverzertifikat auf dem Sitzungsaufzeichnungsserver als vertrauenswürdig einstufen.
- **Inkonsistente Benennung:** Wenn das Serverzertifikat, das dem Computer mit dem Sitzungsaufzeichnungsserver zugewiesen ist, mit einem vollqualifizierten Domänennamen (FQDN) erstellt wurde, müssen alle Komponenten, die eine Verbindung herstellen, für die Verbindung mit dem Sitzungsaufzeichnungsserver den vollqualifizierten Domänennamen verwenden. Wenn ein NetBIOS-Name verwendet wird, konfigurieren Sie die Komponenten mit einem NetBIOS-Namen für den Sitzungsaufzeichnungsserver.
- **Abgelaufene Zertifikate:** Wenn ein Serverzertifikat abgelaufen ist, schlägt eine Verbindung mit dem Sitzungsaufzeichnungsserver über HTTPS fehl. Stellen Sie sicher, dass das Zertifikat, das dem Computer mit dem Sitzungsaufzeichnungsserver zugewiesen ist, gültig und nicht abgelaufen ist. Wenn dasselbe Zertifikat für die digitale Signatur der Sitzungsaufzeichnungen verwendet wird, enthält das Ereignisprotokoll des Computers mit dem Sitzungsaufzeichnungsserver Fehlermeldungen, dass das Zertifikat abgelaufen ist, oder Warnmeldungen, wenn das Zertifikat bald abläuft.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Probleme beim Suchen nach Aufzeichnungen im Sitzungsaufzeichnungsplayer

Jul 08, 2016

Wenn Sie Probleme beim Suchen nach Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

- Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Der Name des Remoteservers konnte nicht aufgelöst werden: Servername. Wobei Servername der Name des Servers ist, mit dem der Sitzungsaufzeichnungsplayer versucht, eine Verbindung herzustellen. Der Sitzungsaufzeichnungsplayer kann den Sitzungsaufzeichnungsserver nicht kontaktieren. Zu den zwei möglichen Gründen gehören ein falsch eingegebener Servername, oder DNS kann den Servernamen nicht auflösen.
  Lösung: Klicken Sie im Player-Menü auf Extras > Optionen > Verbindungen und prüfen Sie die Richtigkeit des Servernamens, der in der Liste Sitzungsaufzeichnungsserver aufgeführt ist. Wenn der Name richtig ist, stellen Sie mit dem Ping-Befehl sicher, dass der Name aufgelöst werden kann. Wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist, tritt ein Fehler beim Suchen nach Sitzungsaufzeichnungsdateien auf. Die Fehlermeldung lautet Fehler beim Verbinden mit dem Remoteserver.

- Fehler beim Verbinden mit dem Remoteserver: Dieser Fehler tritt auf, wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist.
  Lösung: Stellen Sie sicher, dass der Sitzungsaufzeichnungsserver verbunden ist.

- Fehler: Zugriff verweigert. Ein Fehler "Zugriff verweigert" kann auftreten, wenn der Benutzer nicht berechtigt ist, Sitzungsaufzeichnungsdateien zu suchen und herunterzuladen.
  Lösung: Weisen Sie den Benutzer in der Sitzungsaufzeichnungs-Autorisierungskonsole der Rolle "Player" zu.

- Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Die zugrunde liegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden. Diese Ausnahme tritt auf, wenn der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer Zertifizierungsstelle signiert ist, die das Clientgerät nicht vertrauenswürdig ansieht oder für die das Clientgerät kein Zertifikat der Zertifizierungsstelle hat.
  Lösung: Installieren Sie das richtige oder vertrauenswürdige Zertifikat der Zertifizierungsstelle auf der Arbeitsstation, auf der der Sitzungsaufzeichnungsplayer installiert ist.

- Der Remoteserver gaben einen Fehler zurück: (403) verboten. Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres Protokoll) versuchen. Der Server lehnt die Verbindung ab, da er standardmäßig nur sichere Verbindungen annimmt.
  Lösung: Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf Extras > Optionen > Verbindungen. Wählen Sie den Server aus der Liste Sitzungsaufzeichnungsserver aus und klicken Sie auf Ändern. Ändern Sie das Protokoll von HTTP in HTTPS.

## Problembehandlung bei MSMQ

Wenn den Benutzern eine Benachrichtigung angezeigt wird, der Benutzer die Aufzeichnungen jedoch nicht nach dem Durchführen einer Suche im Sitzungsaufzeichnungsplayer finden kann, kann ein Problem mit MSMQ bestehen. Stellen Sie sicher, dass die Warteschlange mit dem Sitzungsaufzeichnungsserver (Speichermanager) verbunden ist. Testen Sie mit einem Webbrowser, ob Verbindungsfehler bestehen (wenn Sie HTTP oder HTTPS als MSMQ-Kommunikationsprotokoll verwenden).


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sicherstellen der Verbindung der Warteschlange

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent gehostet wird, und zeigen Sie die ausgehenden Warteschlangen an.
2. Stellen Sie sicher, dass die Warteschlange des Computers mit dem Sitzungsaufzeichnungsserver verbunden ist.
   - Wenn der Zustand **Warten auf Verbindung** ist, mehrere Nachrichten in der Warteschlange sind und als Protokoll HTTP oder HTTPS verwendet wird (gemäß Auswahl auf der Registerkarte Verbindungen im Dialogfeld Sitzungsaufzeichnungsagent - Eigenschaften), führen Sie Schritt 3 aus.
   - Wenn der Zustand **Verbunden** ist und keine Nachrichten in der Warteschlange sind, besteht möglicherweise ein Problem mit dem Server, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird. Überspringen Sie Schritt 3 und führen Sie Schritt 4 aus.
3. Wenn mehrere Nachrichten in der Warteschlange sind, starten Sie einen Webbrowser und geben Sie folgende Adresse ein:
   - HTTPS: **https://servername/msmq/private$/CitrixSmAudData**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: **http://servername/msmq/private$/CitrixSmAudData**, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

   Wenn die Seite einen Fehler zurückgibt, z. B. Der Server nimmt nur sichere Verbindungen an, ändern Sie das für MSMQ im Dialogfeld Sitzungsaufzeichnungsagent - Eigenschaften aufgeführte Protokoll in HTTPS. Wird ein Problem mit dem Websitesicherheitszertifikat gemeldet, besteht möglicherweise ein Problem mit der Vertrauensbeziehung für den sicheren Kanal (TLS). Installieren Sie dann das richtige Zertifikat der Zertifizierungsstelle oder verwenden Sie eine vertrauenswürdige Zertifizierungsstelle.

4. Wenn die Warteschlange keine Nachrichten enthält, melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an und zeigen Sie private Warteschlangen an. Wählen Sie citrixsmauddata. Wenn mehrere Nachrichten in der Warteschlange sind (Spalte "Nachrichtenanzahl"), stellen Sie sicher, dass der Dienst des Speichermanagers der Sitzungsaufzeichnung gestartet ist. Starten Sie sonst den Dienst neu.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Ändern des Kommunikationsprotokolls

Jul 08, 2016

Aus Sicherheitsgründen empfiehlt Citrix, HTTP nicht als Kommunikationsprotokoll zu verwenden. Die Sitzungsaufzeichnung ist für die Verwendung von HTTPS konfiguriert. Wenn Sie HTTP statt HTTPS verwenden möchten, müssen Sie mehrere Einstellungen ändern.

## Verwenden von HTTP als Kommunikationsprotokoll

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an und deaktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie das eingestellte Protokoll von HTTPS in HTTP in jedem Dialogfeld Sitzungsaufzeichnungsagent - Eigenschaften:
   1. Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
   2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsagent - Eigenschaften.
   3. Klicken unter "Sitzungsaufzeichnungsagent - Eigenschaften" auf die Registerkarte Verbindungen.
   4. Klicken Sie im Bereich Sitzungsaufzeichnungsbroker in der Dropdownliste Protokoll auf HTTP und bestätigen Sie die Änderung mit OK. Bestätigen Sie den Neustart des Dienstes mit Ja.
3. Ändern Sie die Protokolleinstellung in den Sitzungsaufzeichnungsplayer-Einstellungen von HTTPS in HTTP:
   1. Melden Sie sich bei jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
   2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.
   3. Klicken Sie im Menü von Sitzungsaufzeichnungsplayer auf Extras > Optionen > Verbindungen, wählen Sie den Server aus und klicken Sie auf Ändern.
   4. Wählen Sie HTTP aus der Dropdownliste Protokoll aus und klicken Sie zwei Mal auf OK, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.
4. Ändern Sie die Protokolleinstellung in den Einstellungen der Richtlinienkonsole für die Sitzungsaufzeichnung von HTTPS in HTTP:
   1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
   2. Klicken Sie im Menü Start auf Richtlinienkonsole für die Sitzungsaufzeichnung.
   3. Wählen Sie HTTP aus der Dropdownliste Protokoll und klicken Sie auf OK , um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.

## Zurücksetzen des Kommunikationsprotokolls auf HTTPS

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an und aktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie das eingestellte Protokoll von HTTP in HTTPS in jedem Dialogfeld Sitzungsaufzeichnungsagent - Eigenschaften:
   1. Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
   2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsagent - Eigenschaften.
   3. Klicken unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte Verbindungen.
   4. Klicken Sie im Bereich Sitzungsaufzeichnungsbroker in der Dropdownliste Protokoll auf HTTPS und bestätigen Sie die Änderung mit OK. Bestätigen Sie den Neustart des Dienstes mit Ja.
3. Ändern Sie die Protokolleinstellung in den Sitzungsaufzeichnungsplayer-Einstellungen von HTTP in HTTPS:
   1. Melden Sie sich bei jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
   2. Klicken Sie im Menü Start auf Sitzungsaufzeichnungsplayer.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie im Menü von Sitzungsaufzeichnungsplayer auf Extras > Optionen > Verbindungen, wählen Sie den Server aus und klicken Sie auf Ändern.
4. Wählen Sie HTTPS aus der Dropdownliste Protokoll aus und klicken Sie zwei Mal auf OK, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.

4. Ändern Sie die Protokolleinstellung in den Einstellungen der Richtlinienkonsole für die Sitzungsaufzeichnung von HTTP in HTTPS:
   1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
   2. Klicken Sie im Menü Start auf Richtlinienkonsole für die Sitzungsaufzeichnung.
   3. Wählen Sie HTTPS aus der Dropdownliste Protokoll und klicken Sie auf OK , um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Verweis: Verwalten der Datensätze in der Datenbank

Jul 08, 2016

Das ICLDB-Dienstprogramm (ICA Log database) ist ein Datenbankbefehlszeilenprogramm, mit dem Sie Sitzungsaufzeichnungsdatensätze in der Datenbank manipulieren. Dieses Dienstprogramm wird mit der Sitzungsaufzeichnung im Verzeichnis Laufwerk:\Programme\Citrix\SessionRecording\Server\Bin auf dem Server mit der Serversoftware der Sitzungsaufzeichnung installiert.

## Übersichtstabelle

In der folgenden Tabelle finden Sie die Befehle und Optionen für das ICLDB-Dienstprogramm. Geben Sie die Befehle im folgenden Format ein:

icldb [version | locate | dormant | import | archive | remove | removeall] Befehlsoptionen [/l] [/f] [/s] [/?]

Hinweis: Weitere Informationen finden Sie in der Hilfe des Hilfsprogramms. Zum Öffnen der Hilfe geben Sie an der Eingabeaufforderung Laufwerk:**\%ProgramFiles%\Citrix\SessionRecording\Server\Bin** den Befehl **icldb /?** ein. Hilfe für bestimmte Befehle rufen Sie mit dem Befehl **icldb *Befehl* /?** auf.

| Befehl | Beschreibung |
|---|---|
| archive | Archiviert Sitzungsaufzeichnungsdateien, die älter als der angegebene Speicherzeitraum sind. Archivieren Sie Dateien mit diesem Befehl. |
| dormant | Zählt oder zeigt die Sitzungsaufzeichnungsdateien an, die als inaktiv angesehen werden. Inaktive Dateien sind Sitzungsaufzeichnungen, die aufgrund von Datenverlust nicht abgeschlossen wurden.<br>Verwenden Sie diesen Befehl, wenn Sie den Verdacht haben, dass Sie Daten verlieren. Sie können prüfen, ob die Sitzungsaufzeichnungsdateien für die ganze Datenbank oder nur Aufzeichnungen inaktiv werden, die in der angegebenen Anzahl von Tagen, Stunden oder Minuten aufgezeichnet wurden. |
| import | Importiert Sitzungsaufzeichnungsdateien in die Datenbank für die Sitzungsaufzeichnung. Mit diesem Befehl erstellen Sie die Datenbank neu, wenn Sie Datensätze der Datenbank verlieren.<br><br>Mit diesem Befehl führen Sie auch Datenbanken zusammen (wenn Sie zwei Datenbanken haben, können Sie die Dateien von einer der Datenbanken importieren). |
| locate | Sucht und zeigt den vollständigen Pfad einer Sitzungsaufzeichnungsdatei an. Als Kriterium wird die Datei-ID verwendet.<br>Mit diesem Befehl suchen Sie den Speicherort einer Sitzungsaufzeichnungsdatei.<br><br>Außerdem können Sie mit einer bestimmten Datei prüfen, ob die Datenbank aktuell ist. |
| remove | Entfernt die Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank.<br>Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Befehl | Beschreibung |
| --- | --- |
| | Geben Sie den Speicherzeitraum als Kriterium an.<br>Sie können auch die zugeordnete physische Datei löschen. |
| removeall | Entfernt alle Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank für die Sitzungsaufzeichnung und setzt diese auf den Originalzustand zurück. Die physische Datei wird nicht gelöscht. Sie können diese Dateien jedoch nicht im Sitzungsaufzeichnungsplayer suchen.<br>Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). Gelöschte Verweise können nur von einer Sicherungskopie wieder hergestellt werden. |
| version | Zeigt die Schemaversion der Datenbank für die Sitzungsaufzeichnung an. |
| /l | Protokolliert die Ergebnisse und Fehler im Windows-Ereignisprotokoll. |
| /f | Erzwingt die Ausführung des Befehls ohne Aufforderungen. |
| /s | Unterdrückt die Copyright-Nachricht. |
| /? | Zeigt die Hilfe für die Befehle an. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Hinweise von Dritten

Jul 08, 2016

Die Sitzungsaufzeichnung kann Softwarekomponenten von Drittanbietern enthalten, für die die folgenden Lizenzbedingungen gelten: Diese Liste gilt zu dem angegebenen Datum korrekt. Diese Liste kann sich bei bestimmten Versionen des Produkts ändern und ist möglicherweise nicht komplett. Die Liste wird ohne Mängelgewähr zur Verfügung gestellt. IN DEM NACH DEM ANWENDBAREN RECHT ZULÄSSIGEN UMFANG GEBEN CITRIX UND SEINE LIEFERANTEN KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDEN ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN BEZÜGLICH DER LISTE, DEREN RICHTIGKEIT ODER VOLLSTÄNDIGKEIT ODER DEN AUS DER NUTZUNG ODER VERTEILUNGDER LISTE ERGEHENDEN FOLGEN. DURCH NUTZUNG ODER VERTEILUNG DER LISTE STIMMEN SIE ZU, DASS CITRIX UNTER KEINEN UMSTÄNDEN FÜR SPEZIELLE, DIREKTE, INDIREKTE, ODER FOLGESCHÄDEN ODER JEGLICHE ANDEREN SCHÄDEN HAFTET, DIE AUS DER NUTZUNG ODER VERTEILUNG DIESER LISTE ERWACHSEN.

MMC .NET-Bibliothek

Lizenziert unter Common Public License, Version 1.0


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurationsprotokollierung

Jul 08, 2016

Die Konfigurationsprotokollierung dient zum Erfassen der Sitekonfigurationsänderungen und Administratoraktivitäten in einer Datenbank. Sie können den protokollierten Inhalt folgendermaßen verwenden:

- Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen; das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen
- Bericht über Administratoraktivitäten

Zum Festlegen der Einstellungen für die Konfigurationsprotokollierung, zum Anzeigen der Konfigurationsprotokolle und zum Generieren von HTML- und CSV-Berichten verwenden Sie Citrix Studio. Sie können die Anzeige des Konfigurationsprotokolls durch Datumsbereiche und durch Ergebnisse der Volltextsuche filtern. Ist die verbindliche Protokollierung aktiviert, verhindert sie, dass Änderungen an der Konfiguration vorgenommen werden, es sei denn diese können protokolliert werden. Mit der entsprechenden Berechtigung können Sie Einträge aus dem Konfigurationsprotokoll löschen. Sie können das Feature der Konfigurationsprotokollierung nicht zum Bearbeiten des Inhalts von Protokollen verwenden.

Die Konfigurationsprotokollierung verwendet ein PowerShell 2.0-SDK und den Konfigurationsprotokollierungsdienst. Der Konfigurationsprotokollierungsdienst wird auf allen Controllern in der Site ausgeführt. Wenn ein Controller ausfällt, übernimmt automatisch der Dienst auf einem anderen Controller die Verarbeitung von Protokollanforderungen.

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und verwendet die Datenbank, die zusammen mit der Site erstellt wurde (die Sitekonfigurationsdatenbank). Citrix empfiehlt dringend, den Speicherort der Datenbank für die Konfigurationsprotokollierung so schnell wie möglich nach der Erstellung einer Site zu ändern. Die Konfigurationsprotokollierungsdatenbank unterstützt dieselben Features für hohe Verfügbarkeit wie die Sitekonfigurationsdatenbank.

Der Zugriff auf die Konfigurationsprotokollierung wird über die delegierte Administration mit den Einstellungen "Protokollierungseinstellungen bearbeiten" und "Konfigurationsprotokolle anzeigen" gesteuert.

Konfigurationsprotokolle werden bei der Erstellung lokalisiert. Beispiel: Ein in Englisch erstelltes Protokoll wird unabhängig vom Gebietsschema des Lesers in Englisch gelesen.

# Gegenstand der Protokollierung

Konfigurationsänderungen und Administratoraktivitäten, die von Studio, Director und PowerShell-Skripts ausgehen, werden protokolliert. Beispiele protokollierter Konfigurationsänderungen sind Arbeiten (Erstellen, Bearbeiten, Löschen, Zuweisen) mit:

- Maschinenkataloge
- Bereitstellungsgruppen (einschließlich Ändern der Energieverwaltungseinstellungen)
- Administratorrollen und Geltungsbereiche
- Hostressourcen und Verbindungen
- Citrix Richtlinien über Studio

Beispiele protokollierter Administratoraktivitäten:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Energieverwaltung für eine virtuelle Maschine oder einen Benutzerdesktop
- Senden einer Nachricht an einen Benutzer von Studio oder Director aus

Die folgenden Vorgänge werden nicht protokolliert:

- Autonome Vorgänge wie das Einschalten virtueller Maschinen per Poolverwaltung.
- Über die Gruppenrichtlinien-Verwaltungskonsole implementierte Richtlinienaktionen; verwenden Sie Microsoft-Tools, um Protokolle dieser Aktionen anzuzeigen.
- Über die Registrierung vorgenommene Änderungen, direkter Zugriff von der Datenbank oder von anderen Quellen als Studio, Director oder PowerShell.
- Wenn die Bereitstellung initialisiert wird, steht die Konfigurationsprotokollierung ab dem Zeitpunkt zur Verfügung, zu dem die erste Instanz des Konfigurationsprotokollierungsdiensts sich beim Konfigurationsdienst registriert. Daher werden die frühen Phasen der Konfiguration nicht protokolliert (z. B., wenn das Datenbankschema bei der Initialisierung eines Hypervisors abgerufen und angewendet wird).

# Verwalten der Konfigurationsprotokollierung

Standardmäßig wird für die Konfigurationsprotokollierung die Datenbank verwendet, die zusammen mit einer Site erstellt wird (die Sitekonfigurationsdatenbank). Citrix empfiehlt aus folgenden Gründen, einen anderen Speicherort für die Konfigurationsprotokollierungsdatenbank und die Überwachungsdatenbank zu wählen:

- Die Backupstrategie für die Konfigurationsprotokollierungsdatenbank unterscheidet sich wahrscheinlich von der Backupstrategie für die Sitekonfigurationsdatenbank.
- Die Menge der für die Konfigurationsprotokollierung (und den Überwachungsdienst) gesammelten Daten kann den für die Sitekonfigurationsdatenbank verfügbaren Speicherplatz zu stark limitieren.
- Eine einzelne Fehlerquelle für die drei Datenbanken wird beseitigt (d. h. aufgeteilt).

**Hinweis**: Produkteditionen, die keine Konfigurationsprotokollierung unterstützen, haben keinen Knoten namens "Protokollierung" in Studio.

# Aktivieren/Deaktivieren der Konfigurationsprotokollierung und der verbindlichen Protokollierung

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und die verbindliche Protokollierung ist deaktiviert.

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Einstellungen** aus. Das Dialogfeld "Konfigurationsprotokollierung" enthält die Datenbankinformationen und Angaben dazu, ob Konfigurationsprotokollierung und verbindliche Protokollierung aktiviert oder deaktiviert sind.
3. Wählen Sie die gewünschte Aktion:

   Zum Aktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Protokollierung aktivieren**. Dies ist die Standardeinstellung. Wenn nicht in die Datenbank geschrieben werden kann, werden die Informationen verworfen, der


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vorgang wird jedoch fortgesetzt.

Zum Deaktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Protokollierung deaktivieren**. Wenn die Protokollierung zuvor aktiviert war, können bereits vorhandene Protokolle weiterhin mit dem PowerShell-SDK gelesen werden.

Zum Aktivieren der verbindlichen Protokollierung deaktivieren Sie das Kontrollkästchen **Änderungen zulassen, wenn die Verbindung mit der Datenbank getrennt ist**. Es wird dann keine Konfigurationsänderung oder administrative Aktivität, die normalerweise protokolliert würde, zugelassen, es sei denn, sie kann in die Konfigurationsprotokollierungsdatenbank geschrieben werden. Sie können die verbindliche Protokollierung nur aktivieren, wenn die Konfigurationsprotokollierung aktiviert ist, d. h. wenn das Optionsfeld **Protokollierung aktivieren** für die Konfigurationsprotokollierung aktiviert ist. Tritt bei dem Dienst für die Konfigurationsprotokollierung ein Fehler auf, und die hohe Verfügbarkeit wird nicht verwendet, beginnt die verbindliche Protokollierung. In solchen Fällen werden Vorgänge, die normalerweise protokolliert würden, nicht ausgeführt.

Zum Deaktivieren der verbindlichen Protokollierung aktivieren Sie das Kontrollkästchen **Änderungen zulassen, wenn die Verbindung mit der Datenbank getrennt ist**. Konfigurationsänderungen und administrative Aktivitäten sind dann zulässig, selbst wenn kein Zugriff auf die Datenbank für die Konfigurationsprotokollierung besteht. Dies ist die Standardeinstellung.

# Ändern des Speicherorts für die Konfigurationsprotokollierungsdatenbank

**Hinweis:** Sie können den Speicherort der Datenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist, da bei der Standortänderung eine kurze Trennung verursacht wird, die nicht protokolliert werden kann.

1. Erstellen Sie einen Datenbankserver mit einer unterstützten SQL Server-Version.
2. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
3. Wählen Sie im Aktionsbereich **Einstellungen** aus.
4. Klicken Sie im Dialogfeld "Protokollierungseinstellungen" auf **Protokollierungsdatenbank ändern**.
5. Geben Sie im Dialogfeld "Protokollierungsdatenbank ändern" den Speicherort des Servers mit dem neuen Datenbankserver ein. Gültige Formate sind im Artikel "Datenbanken" aufgeführt.
6. Damit die Datenbank von Studio erstellt wird, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK** und die Datenbank wird automatisch erstellt. Studio versucht, mit den Anmeldeinformationen des aktuellen Studio-Benutzers auf die Datenbank zuzugreifen; wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die Datenbank hochgeladen. (Die Anmeldeinformationen werden nur während der Datenbankerstellung gespeichert.)
7. Zum manuellen Erstellen der Datenbank klicken Sie auf **Datenbankskript erstellen**. Das generierte Skript enthält Anweisungen zum manuellen Erstellen der Datenbank. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.

Die Daten der Konfigurationsprotokollierung aus der älteren Datenbank werden nicht in die neue Datenbank importiert. Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden. Der erste Protokolleintrag in der neuen Datenbank für die Konfigurationsprotokollierung gibt an, dass eine Datenbankänderung stattfand; die vorherige Datenbank wird jedoch nicht identifiziert.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Anzeigen des Konfigurationsprotokolls

Beim Initiieren von Konfigurationsänderungen und bei Verwaltungsaktivitäten werden die von Studio und Director bewirkten High-Level-Operationen im oberen mittleren Bereich von Studio angezeigt. Eine High-Level-Operation führt zu mindestens einem Dienst- und SDK-Aufruf, bei dem es sich um eine Low-Level-Operation handelt. Wenn Sie eine High-Level-Operation im oberen mittleren Bereich auswählen, werden im unteren mittleren Bereich die Low-Level-Operationen angezeigt.

Schlägt eine Operation vor der Beendigung fehl, kann die Protokollierung evtl. in der Datenbank nicht abgeschlossen werden, sodass z. B. ein Startdatensatz keinen entsprechenden Stoppdatensatz hat. In solchen Fällen wird im Protokoll angezeigt, dass Informationen fehlen. Wenn Sie Protokolle auf Zeitbereichsbasis anzeigen, werden unvollständige Protokolle angezeigt, wenn die Daten in den Protokollen mit den Kriterien übereinstimmen. Beispiel: Wenn alle Protokolle für die letzten fünf Tage angefordert werden und ein Protokoll eine in den letzten fünf Tagen gelegene Startzeit aber keine Endzeit hat, wird dieses ebenfalls angezeigt.

Wenn Sie bei Verwendung eines Skripts zum Aufrufen von PowerShell-Cmdlets eine Low-Level-Operation erstellen ohne die übergeordnete High-Level-Operation anzugeben, wird von der Konfigurationsprotokollierung eine Ersatz-High-Level-Operation erstellt.

Zum Anzeigen des Inhalts des Konfigurationsprotokolls wählen Sie im Studio-Navigationsbereich **Protokollierung**. Standardmäßig wird im mittleren Bereich der Protokollinhalt chronologisch (neueste Einträge zuerst), angezeigt, wobei die Einträge durch das Datum getrennt sind.

| Zum Filtern der Anzeige nach folgenden Kriterium | Führen Sie folgenden Schritt aus |
|---|---|
| Suchergebnisse | Geben Sie Text in das Feld "Suchen" oben im mittleren Bereich ein. Die gefilterte Anzeige enthält die Anzahl der Suchergebnisse. Zum Zurückkehren zur Standardprotokollanzeige löschen Sie den Text im Feld Suchen. |
| Spaltenüberschrift | Klicken Sie auf eine Spaltenüberschrift, um die Anzeige nach dem entsprechenden Feld zu sortieren. |
| Datumsbereich | Wählen Sie aus der Dropdownliste neben dem Feld "Suchen" oben im mittleren Bereich ein Intervall aus. |

# Erstellen von Berichten

Sie können CSV- und HTML-Berichte mit Konfigurationsprotokolldaten generieren.

- Der CSV-Bericht enthält alle Protokolldaten aus einem angegebenen Zeitintervall. Die hierarchischen Daten in der Datenbank werden in eine einzelne CSV-Tabelle vereinfacht. Kein Aspekt der Daten hat Vorrang in der Datei. Es wird keine Formatierung verwendet und keine Lesbarkeit angenommen. Die Datei (unter dem Namen "MyReport") enthält lediglich die Daten in einem allgemein verwendbaren Format. CSV-Dateien werden oft für die Archivierung oder als Datenquelle für ein Tool zur Bearbeitung von Berichten oder Daten (z. B. Microsoft Excel) verwendet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Der HTML-Bericht enthält Protokolldaten aus einem angegebenen Zeitintervall in lesbarem Format. Er bietet eine strukturierte Ansicht für die Prüfung auf Änderungen, durch die navigiert werden kann. Der HTML-Bericht umfasst zwei Dateien: Zusammenfassung und Details. Die Zusammenfassung enthält High-Level-Operationen mit Informationen zu Zeitpunkt, Auslöser und Ergebnis. Durch Klicken auf den Link Details neben jedem Vorgang navigieren Sie zu den Low-Level-Operationen in der Datei Details, die zusätzliche Informationen bietet.

Zum Generieren eines Konfigurationsprotokollierungsberichts wählen Sie im Studio-Navigationsbereich **Protokollierung** und dann im Aktionsbereich **Benutzerdefinierten Bericht erstellen**.

- Wählen Sie den Datumsbereich für den Bericht.
- Wählen Sie das Berichtsformat: CSV, HTML oder beides.
- Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll.

# Löschen des Konfigurationsprotokolls

Zum Löschen des Konfigurationsprotokolls müssen Sie über bestimmte Rechte der delegierten Administration und Berechtigungen für die SQL Server-Datenbank verfügen.

- **Delegierte Administration**: Sie müssen eine Rolle der delegierten Administration haben, mit der die Bereitstellungskonfiguration gelesen werden kann. Die integrierte Volladministratorrolle hat diese Berechtigung. Für eine benutzerdefinierte Rolle muss für die Kategorie "Andere Berechtigungen" "Lesen" oder "Verwalten" aktiviert sein.
  Wenn Sie die Konfigurationsprotokolldaten vor dem Löschen sichern möchten, muss die benutzerdefinierte Rolle in der Kategorie der Protokollierungsberechtigungen Lese- oder Verwaltungsberechtigung haben.

- **SQL Server-Datenbank**: Sie müssen einen Anmeldenamen für SQL Server haben und zum Löschen von Datensätzen aus der Datenbank berechtigt sein. Dies kann mit zwei Möglichkeiten erreicht werden:
  - Verwenden Sie zur Anmeldung für die SQL Server-Datenbank die Serverrolle "sysadmin", mit der Sie beliebige Aktivitäten auf dem Datenbankserver durchführen können. Auch die Serverrollen "serveradmin" oder "setupadmin" sind zum Löschen von Vorgängen berechtigt.
  - Wenn Ihre Bereitstellung zusätzliche Sicherheit erfordert, verwenden Sie Anmeldeinformationen einer anderen Rolle als "sysadmin", die einem Datenbankbenutzer zugeordnet sind, der zum Löschen von Datensätzen aus der Datenbank berechtigt ist.
    1. Erstellen Sie in SQL Server Management Studio eine SQL Server-Anmeldung mit einer anderen Serverrolle (nicht "sysadmin").
    2. Ordnen Sie diese Anmeldung einem Benutzer in der Datenbank zu; SQL Server erstellt automatisch einen Benutzer in der Datenbank mit dem gleichen Namen wie die Anmeldung.
    3. Geben Sie für die Datenbankrollen-Mitgliedschaft mindestens eines der Rollenmitglieder für den Datenbankbenutzer an: ConfigurationLoggingSchema_ROLE oder dbowner.

    Weitere Informationen finden Sie in der Dokumentation zu SQL Server Management Studio.

Löschen der Konfigurationsprotokolle:

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Protokolle löschen** aus.
3. Sie haben nun die Möglichkeit, vor dem Löschen ein Backup der Protokolle anzulegen. Wenn Sie eine Backupdatei erstellen, navigieren Sie zu dem Speicherort, an dem diese gespeichert werden soll. Das Backup wird als CSV-Datei erstellt.

Nach dem Löschen der Konfigurationsprotokolle wird das Löschen des Protokolls als erste Aktivität im leeren Protokoll


© 1999-2017 Citrix Systems, Inc. All rights reserved.

erfasst. Dieser Eintrag enthält Details darüber, wann und von wem die Protokolle gelöscht wurden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überwachen von Personal vDisks

Jul 08, 2016

Sie können ein Diagnosetool zum Überwachen der Änderungen verwenden, die von Benutzern an beiden Bereichen persönlicher vDisks (Benutzerdaten- und Anwendungsbereiche) vorgenommen werden. Zu diesen Änderungen gehören Anwendungen, die von Benutzern installiert wurden, und von ihnen geänderte Dateien. Die Änderungen werden in einer Reihe von Berichten erfasst.

1. Führen Sie auf der zu überwachenden Maschine **C:\Programme\Citrix\personal vDisk\bin\CtxPvdDiag.exe** aus.
2. Navigieren Sie zu einem Speicherort, an dem die Berichte und Protokolle gespeichert werden sollen, legen Sie fest, welche Berichte generiert werden sollen, und klicken Sie auf **OK**. Die verfügbaren Berichte sind unten aufgeführt.

**Softwarestrukturbericht:** Dieser Bericht generiert die beiden Dateien Software.Dat.Report.txt und Software.Dat.delta.txt.
In Software.Dat.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software" vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of Applications installed on the base: Anwendungen, die auf Ebene 0 installiert wurden
- List of user installed software: Anwendungen, die vom Benutzer im Anwendungsbereich der persönlichen vDisk installiert wurden
- List of software uninstalled by user: ursprünglich auf Ebene 0 installierte Anwendungen, die vom Benutzer entfernt wurden

Weitere Informationen zu Software.Dat.delta.txt finden Sie im Strukturdeltabericht.

**Systemstrukturbericht:** In der Datei SYSTEM.CurrentControlSet.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\System" vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of user installed services: vom Benutzer installierte Dienste und Treiber
- Startup of following services were changed: Dienste und Treiber, deren Starttyp vom Benutzer geändert wurde

**Sicherheitsstrukturbericht:** In der Datei SECURITY.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Security" vorgenommen wurden.

**Strukturbericht für die Sicherheitskontenverwaltung (SAM):** In der Datei SAM.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\SAM" vorgenommen wurden.

**Strukturdeltabericht:** In der Datei Software.Dat.delta.txt werden alle hinzugefügten und entfernten Registrierungsschlüssel und alle Werte erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software" geändert wurden.

**Personal vDisk-Protokolle:** Die Protokolldateien Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log und vDeskService-<#>.log werden standardmäßig im Ordner P:\Users\\AppData\Local\Temp\PVDLOGS erstellt, jedoch an den ausgewählten Speicherort verschoben.

**Windows-Betriebssystemprotokolle**

- EvtLog_App.xml und EvtLog_System.xml sind die Anwendungs- und Systemereignisprotokolle im XML-Format aus dem Personal vDisk-Volume.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Die Protokolle Setupapi.app.log und setuperr.log enthalten Protokollmeldungen bezüglich der Ausführung von msiexec.exe bei der Installation von Personal vDisk.
- Setupapi.dev.log enthält Protokollmeldungen über die Geräteinstallation.
- Msinfo.txt enthält die Ausgabe von msinfo32.exe. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

**Dateisystembericht:** In der Datei FileSystemReport.txt werden die Änderungen erfasst, die vom Benutzer in folgenden Bereichen des Dateisystems vorgenommen wurden:

- Files Relocated: Dateien auf Ebene 0, die vom Benutzer zur vDisk verschoben wurden. Dateien der Ebene 0 sind Dateien, die aus dem Masterimage von der Maschine geerbt wurden, der die persönliche vDisk angefügt ist.
- Files Removed: Dateien auf Ebene 0, die durch eine Benutzeraktion (z. B. Entfernen einer Anwendung) verborgen wurden.
- Files Added (MOF,INF,SYS): Dateien mit der Erweiterung "mof", "inf" oder "sys", die vom Benutzer der Personal vDisk hinzugefügt wurden (z. B. bei der Installation einer Anwendung wie Visual Studio 2010, bei der eine MOF-Datei für die automatische Wiederherstellung registriert wird).
- Files Added Other: Andere Dateien, die der vDisk vom Benutzer hinzugefügt wurden (z. B. beim Installieren einer Anwendung).
- Base Files Modified But Not Relocated: Dateien auf Ebene 0, die vom Benutzer geändert wurden, jedoch nicht von den Personal vDisk-Kernelmodustreibern in der vDisk erfasst wurden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Director

Aug 17, 2016

Dieser Abschnitt enthält folgende Themen:


Info über Director

Bereitstellen und Konfigurieren von Director

Installieren von Director

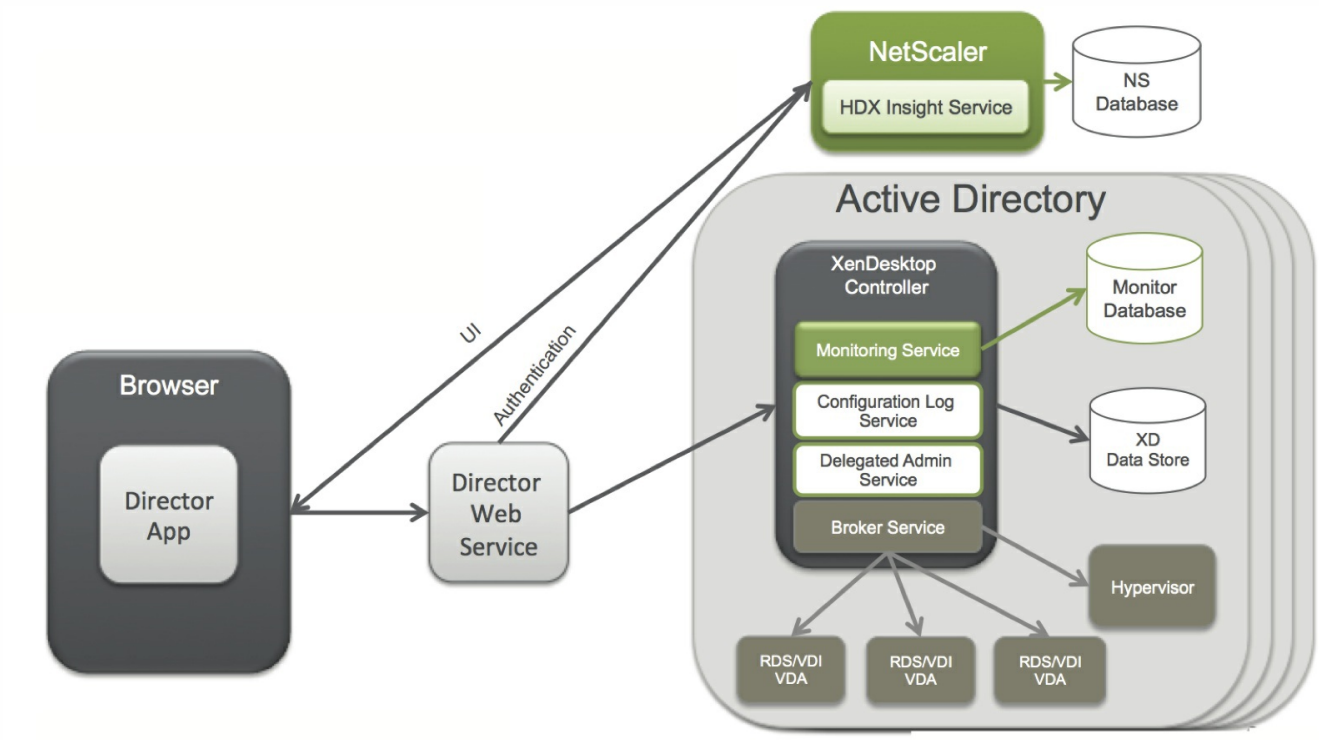
Installieren von Director für XenApp 6.5

Anmelden bei Director

Verwenden von Director mit der integrierten Windows-Authentifizierung


## Info über Director

Director ist ein Echtzeit-Webtool, mit dem Administratoren Endbenutzer überwachen, Fehler beheben und Support leisten können.




Director hat auf Folgendes Zugriff:

- Echtzeitdaten vom Broker Agent über eine einheitliche Konsole, die mit Analytics, Leistungsverwaltung und Netzwerkinspektion integriert ist.
  - Analytics umfasst Leistungsverwaltung zum Sicherstellen von Integrität und Kapazität, sowie historische Trends und Netzwerkanalyse (von NetScaler HDX Insight) zum Identifizieren von Engpässen, die auf dem Netzwerk in der XenApp- oder XenDesktop-Umgebung beruhen.
- In der Überwachungsdatenbank gespeicherte historische Daten für den Zugriff auf die Datenbank für die

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Konfigurationsprotokollierung.
- ICA-Daten von NetScaler Gateway mit HDX Insight.
  - Übersicht über die Endbenutzererfahrung für virtuelle Anwendungen, Desktops und Benutzer in XenApp oder XenDesktop.
  - Korrelation von Netzwerkdaten mit Anwendungsdaten und Echtzeitmetrik für effektive Problembehandlung.
  - Integration mit dem Überwachungstool von XenDesktop 7 Director.
- Personal vDisk-Daten, die die Ausführungsüberwachung anhand von Basiszuordnung und Helpdesk-Mitarbeitern das Zurücksetzen von Personal vDisks ermöglichen (nur im Notfall zu verwenden).
  - Das Befehlszeilentool CtxPvdDiag.exe wird zum Sammeln von Benutzerinformationen in einer Datei zur Problembehandlung verwendet.

Director hat ein Dashboard zur Problembehandlung, das die Echtzeitzustandsüberwachung der XenApp- oder XenDesktop-Site ermöglicht. Mit dieser Funktion können Administratoren Fehler in Echtzeit sehen und einen besseren Eindruck von der Endbenutzererfahrung erhalten.

## Ansichten

Director bietet verschiedene Ansichten der Schnittstelle, die auf bestimmte Administratoren abgestimmt sind. Produktberechtigungen bestimmen, was angezeigt wird und welche Befehle verfügbar sind.

Beispiel: Helpdeskadministratoren sehen eine auf Helpdeskaufgaben abgestimmte Schnittstelle. Director ermöglicht Helpdeskadministratoren, nach dem Benutzer zu suchen, der das Problem gemeldet hat, und die diesem Benutzer zugeordneten Aktivitäten anzuzeigen, z. B. den Status der Anwendungen und Prozesse des Benutzers. So können Probleme schnell gelöst werden, indem Aktionen wie z. B. das Beenden einer nicht reagierenden Anwendung oder eines Prozesses, das Spiegeln von Vorgängen auf der Maschine des Benutzers, der Neustart der Maschine oder das Zurücksetzen des Benutzerprofils durchgeführt werden.

Im Gegensatz dazu sehen und verwalten Volladministratoren die gesamte Website und können Befehle für mehrere Benutzer und Maschinen ausführen. Das Dashboard bietet einen Überblick über die wichtigsten Aspekte einer Bereitstellung, z. B. den Status von Sitzungen und Benutzeranmeldungen und die Infrastruktur der Site. Die Informationen werden jede Minute aktualisiert. Wenn Probleme auftreten, werden automatisch Details zu Anzahl und Art der Fehler angezeigt.

### Bereitstellen und Konfigurieren von Director

Director ist standardmäßig als Website auf dem Delivery Controller installiert. Informationen zu Voraussetzungen und anderen Details finden Sie in der Dokumentation zu den Systemanforderungen für dieses Release.

Dieses Release von Director ist nicht kompatibel mit XenApp-Bereitstellungen vor Version 6.5 und XenDesktop-Bereitstellungen vor Version 7.

Wenn Director in einer Umgebung mit mehreren Sites verwendet wird, synchronisieren Sie die Systemuhren auf allen Servern, auf denen Controller, Director und andere wichtige Kernkomponenten installiert sind. Ansonsten werden die Sites in Director möglicherweise nicht richtig angezeigt.

Tipp: Wenn Sie beabsichtigen, neben XenApp 7.5- und XenDesktop 7.x-Sites auch XenApp 6.5-Sites zu überwachen, empfiehlt Citrix, Director und die Director-Konsole, die zur Überwachung von XenApp 6.5-Sites verwendet wird, auf separaten Servern zu installieren.
Wichtig: Zum Schutz von als Nur-Text über das Netzwerk gesendeten Benutzernamen und Kennwörtern empfiehlt Citrix dringend, nur Director-Verbindungen mit HTTPS und nicht mit HTTP zuzulassen. Bestimmte Tools können Nur-Text-

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Benutzernamen und -Kennwörter in (unverschlüsselten) HTTP-Netzwerkpaketen lesen, wodurch ein Sicherheitsrisiko für Benutzer entsteht.

**Konfigurieren von Berechtigungen**

Um eine Anmeldung bei Director vornehmen zu können, müssen Administratoren mit den Berechtigungen für Director Active Directory-Domänenbenutzer sein und die folgenden Berechtigungen haben:

- Leseberechtigungen in allen zu durchsuchenden Active Directory-Gesamtstrukturen (siehe Erweiterte Konfiguration)
- Konfigurierte delegierte Administratorrollen (siehe Delegierte Administration und Director)
- Zum Spiegeln von Benutzern muss für Administratoren eine Microsoft-Gruppenrichtlinie für Windows-Remoteunterstützung konfiguriert werden. Darüber hinaus gilt Folgendes:
  - Bei der Installation von VDAs stellen Sie sicher, dass die Windows-Remoteunterstützung auf allen Benutzergeräten aktiviert ist (standardmäßig aktiviert).
  - Wenn Sie Director auf einem Server installieren, stellen Sie sicher, dass die Windows-Remoteunterstützung installiert ist (standardmäßig ausgewählt). Allerdings ist sie auf dem Server standardmäßig deaktiviert. Das Feature muss für Director nicht aktiviert werden, um Benutzern zu helfen. Citrix empfiehlt, das Feature deaktiviert zu lassen, um die Sicherheit auf dem Server zu erhöhen.
  - Damit Administratoren die Windows-Remoteunterstützung initiieren können, müssen Sie ihnen mit den entsprechenden Einstellungen der Microsoft-Gruppenrichtlinie die Berechtigungen für die Remoteunterstützung erteilen. Informationen finden Sie unter CTX127388: How to Enable Remote Assistance for Desktop Director.
- Bei Benutzergeräten mit VDA-Versionen vor 7 ist eine zusätzliche Konfiguration erforderlich. Siehe Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7.

## Installieren von Director

Installieren Sie Director mit dem Produktinstallationsprogramm für XenApp und XenDesktop. Dieses prüft, ob die Voraussetzungen erfüllt sind, installiert fehlende Komponenten, richtet die Director-Website ein und führt die Grundkonfiguration durch. Die Standardkonfiguration, die der Installer bietet, eignet sich für typische Bereitstellungen. Fügen Sie Director mit dem Installationsprogramm hinzu, falls dies während der Installation nicht geschehen ist. Zum Hinzufügen zusätzlicher Komponenten führen Sie den Installer erneut aus und wählen Sie die zu installierenden Komponenten aus. Informationen zur Verwendung des Installationsprogramms finden Sie unter Installieren über die grafische Oberfläche in der Installationsdokumentation. Citrix empfiehlt, dass Sie die Installation ausschließlich mit dem Installer des Produkts und nicht über die MSI-Datei durchführen.

Wenn Director auf dem Controller installiert ist, erfolgt automatisch eine Konfiguration mit "localhost" als Serveradresse und Director kommuniziert standardmäßig mit dem lokalen Controller.

Zur Installation von Director auf einem dedizierten, Controller-remoten Server werden Sie zur Eingabe des FQDN oder der IP-Adresse eines Controllers aufgefordert. Director kommuniziert standardmäßig mit diesem angegebenen Controller. Geben Sie nur eine Controlleradresse für jede zu überwachende Site ein. Director ermittelt automatisch alle anderen Controller in derselben Site und wechselt zu diesen anderen Controllern, wenn der von Ihnen angegebene Controller ausfällt.

**Hinweis:** Director führt keinen Lastausgleich zwischen Controllern aus.

Citrix empfiehlt die Implementierung von TLS auf der IIS-Website, die Director hostet, um die Kommunikation zwischen dem Browser und dem Webserver zu schützen. In der Dokumentation von Microsoft zu IIS finden Sie entsprechende Anweisungen. Zum Aktivieren von TLS ist keine Director-Konfiguration erforderlich.

## Installieren von Director für XenApp 6.5


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Führen Sie die folgenden Schritte aus, um Director für XenApp 6.5 zu installieren. In der Regel wird Director auf einem anderen Computer als die XenApp-Controller installiert.

1. Installieren Sie Director von dem XenApp-Installationsmedium. Wenn Director bereits für XenDesktop installiert ist, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten Schritt fort.
2. Verwenden Sie die IIS-Verwaltungskonsole auf jedem Director-Server, um die Liste der XenApp-Serveradressen in den Anwendungseinstellungen zu aktualisieren (siehe Abschnitt "Hinzufügen von Sites zu Director" im Artikel Erweiterte Konfiguration).
   Geben Sie pro XenApp-Site die Serveradresse eines Controllers an: Die anderen Controller in einer XenApp-Site werden dann automatisch zum Failover verwendet. Director führt keinen Lastausgleich zwischen Controllern aus.

   **Wichtig:** Stellen Sie bei XenApp-Adressen sicher, dass Sie die Einstellung "Service.AutoDiscoveryAddressesXA" und nicht die Standardeinstellung "Service.AutoDiscoveryAddresses" verwenden.
3. Der Installer für den WMI Provider von Director ist auf der DVD im Ordner **Support\DirectorWMIProvider**. Installieren Sie ihn auf den jeweiligen XenApp-Servern (Controller und Worker, wenn Sitzungen ausgeführt werden).
   Wenn **winrm** nicht konfiguriert ist, führen Sie den Befehl **winrm qc** aus.
4. Konfigurieren Sie jeden XenApp-Workerserver für die Annahme von WinRM-Abfragen, wie unter Konfigurieren von Berechtigungen beschrieben.
5. Konfigurieren Sie eine Firewallausnahme für Port 2513, der für die Kommunikation zwischen Director und XenApp verwendet wird.
6. Citrix empfiehlt die Implementierung von TLS auf der IIS-Website, die Director hostet, um die Kommunikation zwischen dem Browser und dem Webserver zu schützen.
   In der Dokumentation von Microsoft zu IIS finden Sie entsprechende Anweisungen. Zum Aktivieren von TLS ist keine Director-Konfiguration erforderlich.

> **Hinweis**
>
> Damit Director alle XenApp-Worker in der Farm findet, müssen Sie eine Reverse-DNS-Zone für die Subnetze hinzufügen, in denen sich die XenApp-Server auf den von der Farm verwendeten DNS-Servern befinden.

### Anmelden bei Director

Die Director-Website ist unter https oder http:///Director.

Wenn eine der Sites einer Bereitstellung mit mehreren Sites ausfällt, dauert die Anmeldung für Director etwas länger, während Verbindungsversuche mit dieser Site laufen.

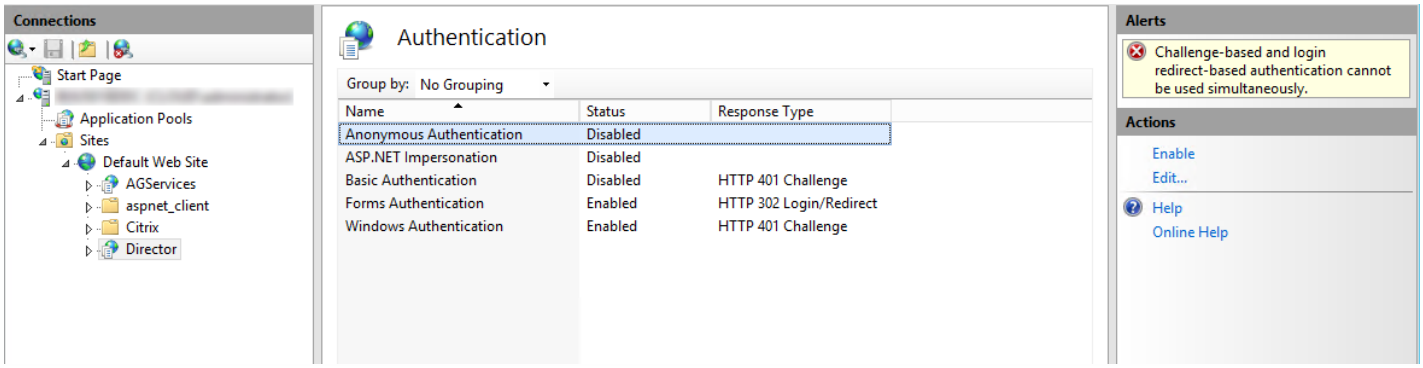
### Verwenden von Director mit der integrierten Windows-Authentifizierung

Mit der integrierten Windows-Authentifizierung erhalten in die Domäne eingebundene Benutzer direkten Zugriff auf Director, ohne ihre Anmeldeinformationen auf der Director-Anmeldeseite erneut eingeben zu müssen. Für die Verwendung der integrierten Windows-Authentifizierung mit Director gelten folgende Voraussetzungen:

- Die integrierte Windows-Authentifizierung muss auf der IIS-Website, die Director hostet, aktiviert werden. Bei der Installation von Director sind Formularauthentifizierung und anonyme Authentifizierung aktiviert. Zur Verwendung der integrierten Windows-Authentifizierung mit Director deaktivieren Sie die anonyme Authentifizierung und aktivieren Sie die Windows-Authentifizierung. Die Formularauthentifizierung sollte für die Authentifizierung domänenexterner Benutzer aktiviert bleiben.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Starten Sie IIS-Manager.
2. Rufen Sie **Sites** > **Standardwebsite** > **Director** auf.
3. Wählen Sie **Authentifizierung**.
4. Klicken Sie mit der rechten Maustaste auf **Anonyme Authentifizierung** und wählen Sie **Deaktivieren**.
5. Klicken Sie mit der rechten Maustaste auf **Windows-Authentifizierung** und wählen Sie **Aktivieren**.




- Konfigurieren Sie die Active Directory-Delegierungsberechtigung für den Director-Computer. Dies ist nur erforderlich, wenn Director und Delivery Controller auf separaten Computern installiert sind.
  1. Öffnen Sie auf dem Active Directory-Computer die Active Directory-Verwaltungskonsole.
  2. Navigieren Sie in der Active Directory-Verwaltungskonsole zu **Domänenname** > **Computer** und wählen Sie den Director-Computer zum Zuweisen der Delegierungsberechtigung.
  3. Klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**.
  4. Wählen Sie die Registerkarte **Delegierung**.
  5. Wählen Sie die Option **Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)**.

- Der Browser, der für den Zugriff auf Director verwendet wird, muss die integrierte Windows-Authentifizierung unterstützen. Dies erfordert möglicherweise zusätzliche Konfigurationsschritte in Firefox und Chrome. Weitere Informationen finden Sie in der Dokumentation zu dem Browser.
- Der Überwachungsdienst muss Microsoft .NET Framework 4.5.1 oder höher ausführen (unterstützte Versionen siehe Systemanforderungen für Director). Weitere Informationen finden Sie unter Systemanforderungen.

Wenn sich ein Benutzer von Director abmeldet oder ein Sitzungstimeout auftritt, wird die Anmeldeseite angezeigt. Auf der Anmeldeseite kann der Benutzer den Authentifizierungstyp auf **Automatische Anmeldung** oder **Benutzeranmeldeinformationen** festlegen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Erweiterte Konfiguration

Jul 08, 2016

Dieser Abschnitt enthält folgende Themen:

Unterstützen von Benutzern in mehreren Active Directory-Domänen und -Gesamtstrukturen

Hinzufügen von Sites zu Director

Deaktivieren der Sichtbarkeit von ausgeführten Anwendungen im Aktivitätsmanager

Einige Elemente der erweiterten Director-Konfigurationen, z. B. die Unterstützung mehrerer Sites oder mehrerer Active Directory-Gesamtstrukturen, wird durch die Einstellungen im Internetinformationsdienste-Manager (IIS) gesteuert.
Wichtig: Wenn Sie eine Einstellung in IIS ändern, wird der Director-Dienst automatisch neu gestartet und die Benutzer werden abgemeldet.
Konfigurieren von erweiterten Einstellungen mit IIS

1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wechseln Sie zur Director-Website unter der Standardwebsite.
3. Doppelklicken Sie auf **Anwendungseinstellungen**.
4. Doppelklicken Sie auf eine Einstellung, um diese zu bearbeiten.

Platinum-Lizenzen behalten Daten standardmäßig 90 Tage lang bei. Weitere Informationen zu Konfigurationen finden Sie unter Datengranularität und -beibehaltung.

## Unterstützen von Benutzern in mehreren Active Directory-Domänen und -Gesamtstrukturen

Director sucht in Active Directory nach Benutzern und nach zusätzlichen Benutzer- und Maschineninformationen. Standardmäßig durchsucht Director die folgende Domäne oder Gesamtstruktur:

- In der das Konto des Administrators Mitglied ist
- In der der Director-Webserver Mitglied ist (falls unterschiedlich)

Director versucht, Suchen auf Gesamtstrukturebene mit dem globalen Active Directory-Katalog durchzuführen Wenn der Administrator keine Berechtigungen zum Suchen auf der Gesamtstrukturebene hat, wird nur die Domäne durchsucht.

Für die Suche nach Daten aus einer anderen Active Directory-Domäne oder Gesamtstrukturebene müssen Sie explizit die zu durchsuchenden Domänen oder Gesamtstrukturen festlegen. Konfigurieren Sie die folgenden Einstellungen:
Connector.ActiveDirectory.Domains = (user),(server)
Die Werte der Attribute Benutzer und Server stellen die Domänen des Director-Benutzers (Administrator) bzw. des Director-Servers dar.

Um Suchen von einer zusätzlichen Domäne oder Gesamtstruktur zu ermöglichen, fügen Sie, wie in diesem Beispiel gezeigt, den Namen der Domäne der Liste hinzu:

Connector.ActiveDirectory.Domains = (user),(server),,
Director versucht, Suchen für jede Domäne in der Liste auf der Gesamtstrukturebene durchzuführen. Wenn der Administrator keine Berechtigungen zum Suchen auf der Gesamtstrukturebene hat, wird nur die Domäne durchsucht.

> Hinweis

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

> In einer Umgebung mit mehreren Gesamtstrukturen zeigt Director nicht die Sitzungsdetails von Benutzern anderer Gesamtstrukturen an, die der XenDesktop-Bereitstellungsgruppe mit der lokalen Gruppe der Domäne zugewiesen wurden.

## Hinzufügen von Sites zu Director

Wenn Director bereits installiert ist, richten Sie das Programm für die Arbeit mit mehreren Sites ein. Verwenden Sie hierzu die IIS-Manager-Konsole auf jedem Director-Server zum Aktualisieren der Liste der Serveradressen in den Anwendungseinstellungen.

Fügen Sie folgender Einstellung eine Controller-Adresse von jedem Standort hinzu:
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
wobei SiteAController und SiteBController die Adressen von XenDesktop-Controllern zweier verschiedener Sites sind.

Fügen Sie bei XenApp 6.5-Sites der folgenden Einstellung eine Controller-Adresse von den jeweiligen XenApp-Farmen hinzu:
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
wobei FarmAController und FarmBController die Adressen von XenApp-Controllern von zwei verschiedenen Farmen sind.

Dies ist eine weitere Methode für XenApp 6.5-Sites, einen Controller von einer XenApp-Farm hinzuzufügen:
DirectorConfig.exe /xenapp FarmControllerName

## Deaktivieren der Sichtbarkeit von ausgeführten Anwendungen im Aktivitätsmanager

Standardmäßig wird im Aktivitätsmanager von Director eine Liste aller ausgeführten Anwendungen für die Benutzersitzung angezeigt. Diese Informationen können von allen Administratoren angezeigt werden, die Zugriff auf den Aktivitätsmanager in Director haben. Bei delegierten Administratorrollen sind dies Volladministratoren, Bereitstellungsgruppenadministratoren und Helpdeskadministratoren.

Zum Schutz der Privatsphäre im Hinblick auf Benutzer und die von ihnen ausgeführten Anwendungen können Sie die Auflistung der ausgeführten Anwendungen auf der Registerkarte "Anwendungen" deaktivieren.

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Ändern Sie für den VDA den Registrierungsschlüssel in HKLM\Software\Citrix\Director\TaskManagerDataDisplayed. Standardmäßig ist dieser Schlüssel auf 1 eingestellt. Ändern Sie den Wert auf 0, was bedeutet, dass die Informationen nicht im Aktivitätsmanager angezeigt werden.
2. Bearbeiten Sie auf dem Server, auf dem Director installiert ist, die Einstellung zur Steuerung der Sichtbarkeit ausgeführter Anwendungen. In der Standardeinstellung ist der Wert "Wahr", wodurch die Sichtbarkeit der ausgeführten Anwendungen auf der Registerkarte Anwendungen zugelassen wird. Ändern Sie den Wert in "Falsch", wodurch die Sichtbarkeit deaktiviert wird. Diese Option gilt nur für den Aktivitätsmanager in Director, nicht für den VDA.
   Ändern Sie den Wert der folgenden Einstellung:
   UI.TaskManager.EnableApplications = false

Wichtig: Zum Deaktivieren der Ansicht ausgeführter Anwendungen empfiehlt Citrix, dass beide Änderungen durchgeführt werden, damit die Daten im Aktivitätsmanager nicht angezeigt werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überwachen von Bereitstellungen

Jul 11, 2016

Dieser Abschnitt enthält folgende Themen:


Überwachen von Sites

Überwachen von Sitzungen

Filtern von Daten zur Problembehandlung

Siteübergreifendes Überwachen von Verlaufstrends

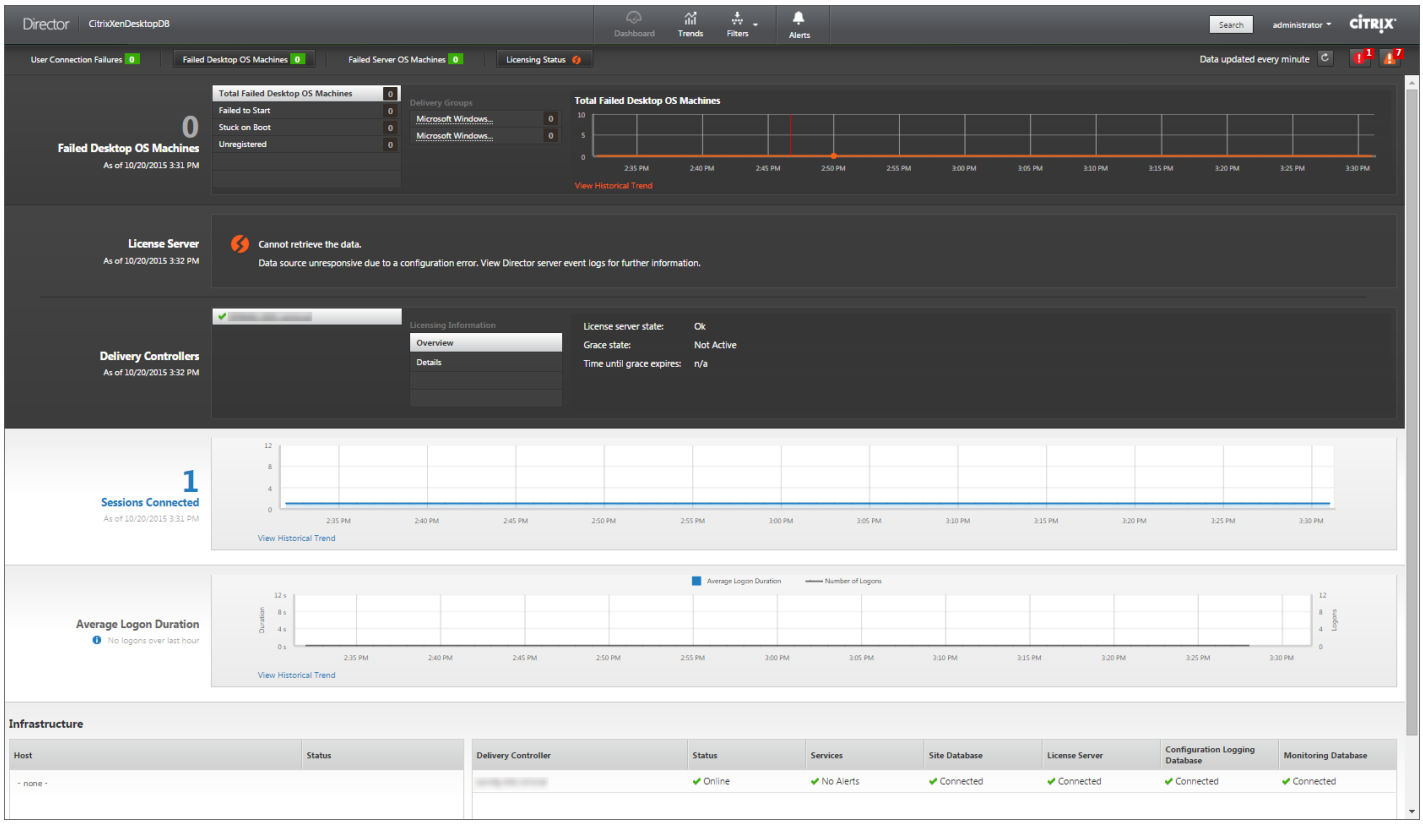
Überwachen von Hotfixes

Steuern der Energiezustände von Benutzermaschinen

Verhindern von Verbindungen mit Maschinen


## Überwachen von Sites

Wenn Sie Director mit Volladministratorrechten öffnen, erscheint das Dashboard zur Überwachung der Integrität und Nutzung einer Site.




Wenn es zurzeit keine Fehler gibt und keine Fehler in den letzten 60 Minuten aufgetreten sind, bleiben Bereiche ausgeblendet. Wenn Fehler auftreten, wird der zugehörige Fehlerbereich automatisch angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hinweis: Je nachdem, über welche Lizenzierung Ihre Organisation verfügt und welche Administratorrechte vorliegen, stehen einige Optionen oder Features möglicherweise nicht zur Verfügung.

| Bereich | Beschreibung |
|---|---|
| Benutzerverbindungsfehler | Verbindungsfehler während der letzten 60 Minuten. Klicken Sie auf die Kategorien neben der Gesamtzahl zum Anzeigen von Metriken für diesen Fehlertyp. In der nebenstehenden Tabelle wird angezeigt, wie sich dieser Wert auf die Bereitstellungsgruppen verteilt. Verbindungsfehler umfassen auch solche, die aufgrund von Anwendungslimits auftreten. Weitere Informationen zu Anwendungslimits finden Sie unter Anwendungen. |
| Fehlgeschlagene Desktopbetriebssystemmaschinen bzw. Fehlgeschlagene Serverbetriebssystemmaschinen | Gesamtanzahl der Fehler in den letzten 60 Minuten unterteilt nach Bereitstellungsgruppen. Fehler unterteilt nach Typ, einschließlich "konnte nicht gestartet werden", "beim Starten hängen geblieben" und "nicht registriert". Bei Serverbetriebssystemmaschinen wird auch das Erreichen der maximalen Last angegeben. |
| Lizenzierungsstatus | • Lizenzserverwarnungen werden vom Lizenzserver gesendet und enthalten für eine Auflösung der jeweiligen Warnung erforderlichen Aktionen.<br>• Delivery Controller-Warnungen enthalten vom Controller erfasste Zustandsangaben zur Lizenzierung und werden vom Delivery Controller gesendet.<br><br>Sie können den Schwellenwert für Warnungen in Studio festlegen.<br><br>Lizenzserver- bzw. Delivery Controller-Warnungen werden nicht angezeigt, wenn die Lizenzserverversion älter ist 11.12.1 bzw. wenn die Delivery Controller-Version älter ist als XenApp 7.6 oder XenDesktop 7.6. |
| Verbundene Sitzungen | Verbunden Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten. |
| Durchschnittliche Anmeldedauer | Anmeldedaten für die letzten 60 Minuten. Die große Zahl links ist die durchschnittliche Anmeldedauer während einer Stunde.<br>Anmeldedaten für VDAs vor XenDesktop 7.0 sind nicht in diesem Durchschnitt enthalten.<br><br>Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen. |
| Infrastruktur | Integritätsstatus der Hosts, Controller und Infrastruktur. Anzeige von Leistungswarnungen.<br>Für Hosts werden der Verbindungsstatus sowie der Zustand der CPU, Arbeitsspeicher, Bandbreite (Netzwerkverwendung) und Speicher (Datenträgernutzung) anhand von Informationen von XenServer oder VMware überwacht.<br><br>Sie können beispielsweise XenCenter so konfigurieren, dass Warnungen zur |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Bereich | Beschreibung |
| --- | --- |
| | Leistung generiert werden, wenn die CPU-, Netzwerk-E/A- oder Datenträger-E/A-Nutzung einen angegebenen Schwellenwert auf einem verwalteten Server oder einer virtuellen Maschine übersteigt. Standardmäßig ist das Warnungswiederholungsintervall 60 Minuten, Sie können jedoch auch eine andere Einstellung wählen. Weitere Informationen finden Sie in der XenServer-Dokumentation unter Konfigurieren von Leistungswarnungen. |

Hinweis: Wird für eine bestimmte Metrik kein Symbol angezeigt, bedeutet dies, dass diese Metrik von dem verwendeten Hosttyp nicht unterstützt wird. Beispiel: Für System Center Virtual Machine Manager-, AWS- und CloudStack-Hosts sind keine Integritätsdaten verfügbar.
Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine
- Verhindern von Verbindungen mit Maschinen

## Überwachen von Sitzungen

Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

| Aktion | Beschreibung |
| --- | --- |
| Anzeigen einer zurzeit verbundenen Maschine oder Sitzung des Benutzers | Mit den Ansichten Aktivitäts-Manager und Benutzerdetails zeigen Sie die aktuell verbundene Maschine oder Sitzung des Benutzers an und eine Liste aller Maschinen und Sitzungen, auf die dieser Benutzer zugreifen kann. Klicken Sie auf das Symbol zum Sitzungswechsel in der Titelleiste des Benutzers, um auf diese Liste zuzugreifen. Siehe Wiederherstellen von Sitzungen. |
| Anzeigen der Gesamtanzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen | Im Dashboard im Bereich Verbundene Sitzungen zeigen Sie die Gesamtzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten an. Wenn Sie anschließend auf die Gesamtzahl klicken, wird die Ansicht Filter angezeigt, in der Sie die grafischen Sitzungsdaten basierend auf ausgewählten Bereitstellungsgruppen und Bereichen und Nutzung von Bereitstellungsgruppen anzeigen. |
| Anzeigen der Daten über einen längeren Zeitraum | Klicken Sie in der Ansicht Trends auf die Registerkarte Sitzungen, um detailliertere Nutzungsdaten für verbundene und getrennte Sitzungen über einen längeren Zeitraum anzuzeigen (d. h. Sitzungsgesamtanzahl, die länger als 60 Minuten zurückliegt). Klicken Sie zum Anzeigen dieser Informationen auf Verlaufstrends anzeigen. |

Hinweis: Wenn auf dem Benutzergerät eine ältere Virtual Delivery Agent-Version ausgeführt wird, z. B. eine VDA-Version vor 7 oder ein VDA für Linux, kann Director keine vollständigen Sitzungsinformationen anzeigen. Stattdessen wird gemeldet, dass die Informationen nicht verfügbar sind.

## Filtern von Daten zur Problembehandlung

Wenn Sie auf Zahlen im Dashboard klicken oder im Menü Filter einen vordefinierten Filter auswählen, wird die Ansicht Filter geöffnet und zeigt Daten für die ausgewählte Maschine oder den Fehlertyp an.

Vordefinierten Filter können nicht bearbeitet werden. Sie können einen vordefinierten Filter jedoch als benutzerdefinierten


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filter speichern und dann bearbeiten. Sie können auch benutzerdefinierten Ansichten mit Filter für Maschinen, Verbindungen und Sitzungen für alle Bereitstellungsgruppen erstellen.

1. Wählen Sie eine Ansicht aus:
   - **Maschinen**: Wählen Sie Desktopbetriebssystemmaschinen oder Serverbetriebssystemmaschinen. Diese Ansicht zeigt die Anzahl der konfigurierten Computer. Die Registerkarte "Serverbetriebssystemmaschinen" enthält auch den Lastauswertungsprogrammindex, der die Verteilung der Leistungsindikatoren und Quickinfo der Sitzungsanzahl angibt, wenn Sie mit dem Mauszeiger auf den Link zeigen.
   - **Sitzungen**: Sie können die Sitzungsanzahl auch in der Ansicht "Maschinen" anzeigen.
   - **Verbindungen**: Filtern Sie Verbindungen nach verschiedenen Zeiträumen, u. a. die letzten 60 Minuten, die letzten 24 Stunden, oder die letzten 7 Tage.
2. Wählen Sie für "Fehler" die Kriterien aus.
3. Verwenden Sie die zusätzlichen Registerkarten für jede Ansicht ggf. zum Abschließen des Filters.
4. Wählen Sie zusätzliche Spalten bei Bedarf aus, um weitere Fehler zu beheben.
5. Speichern und benennen Sie den Filter.
   Wenn Sie den Filter später öffnen möchten, wählen Sie im Menü Filter den Filtertyp (Maschinen, Sitzungen oder Verbindungen) und dann den gespeicherten Filter.

6. Verwenden Sie u. U. für die Ansichten "Maschinen" oder "Verbindungen" für alle in der gefilterten Liste ausgewählten Maschinen Energiesteuerelemente aus. Verwenden Sie in der Ansicht "Sitzungen" die Sitzungssteuerelemente oder die Option zum Senden von Nachrichten.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine

- Verhindern von Verbindungen mit Maschinen

## Siteübergreifendes Überwachen von Verlaufstrends

Die Ansicht "Trends" zeigt Verlaufstrenddaten für Sitzungen, Verbindungsfehler, Maschinenfehler, Anmeldeleistung und Lastauswertung für jede Site an. Klicken Sie zur Anzeige dieser Informationen im Dashboard oder in der Anzeige "Filter" auf "Trends".

Das Vergrößerungsfeature beim Drilldown ermöglicht Ihnen das Navigieren durch Trenddiagramme, indem Sie bestimmte Zeiträume vergrößern (durch Klicken auf einen Datenpunkt im Diagramm) und die Detailinformationen zum Trend anzeigen. Durch dieses Feature können Sie die genauen Auswirkungen der angezeigten Trends besser verstehen.

Wenden Sie einen anderen Filter auf die Daten an, um den Standardgeltungsbereich der einzelnen Diagramme zu ändern.

| **Aktion** | **Beschreibung** |
|---|---|
| Graphdaten exportieren | Wählen Sie die Registerkarte aus, die die Daten enthält, die Sie exportieren möchten. Klicken Sie auf "Exportieren" und wählen Sie das Format: PDF oder CVS. |
| Trends für Sitzungen anzeigen | Wählen Sie auf der Registerkarte "Sitzungen" die Bereitstellungsgruppe und den Zeitraum aus, um weitere Informationen zur Anzahl gleichzeitiger Sitzungen anzuzeigen. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Trends für Verbindungsfehler anzeigen | Wählen Sie auf der Registerkarte "Verbindungsfehler" den Maschinentyp, den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Verbindungsfehler der Site anzuzeigen. |
| Trends für Maschinenfehler anzeigen | Wählen Sie auf der Registerkarte "Desktopbetriebssystemmaschinenfehler" bzw. "Serverbetriebssystemmaschinen" den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Maschinenfehler der Site anzuzeigen. |
| Trends für die Anmeldeleistung anzeigen | Wählen Sie auf der Registerkarte "Anmeldeleistung" die Bereitstellungsgruppe und den Zeitraum, um ein Diagramm mit ausführlichen Informationen über die Dauer der Benutzeranmeldungen bei der Site und wie sich die Anzahl der Anmeldungen auf die Leistung auswirkt, anzuzeigen. In dieser Ansicht wird auch die durchschnittliche Dauer der Anmeldephasen angezeigt, u. a. Vermittlungsdauer, VM-Startzeit usw.<br><br>Diese Daten beziehen sich speziell auf Benutzeranmeldungen und nicht auf Benutzer, die sich mit getrennten Sitzungen wiederverbinden.<br><br>In der Tabelle unterhalb des Diagramms wird die Anmeldedauer nach Benutzersitzung angezeigt. Der Administrator kann die Spalten für die Anzeige auswählen und den Bericht nach einer beliebigen Spalte sortieren.<br><br>Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen. |
| Trends für die Lastauswertung anzeigen | Die Registerkarte "Lastauswertungsindex" bietet ein Diagramm, das ausführliche Informationen zur Last enthält, die auf die Serverbetriebssystemmaschinen verteilt ist. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Serverbetriebssystemmaschine in einer Bereitstellungsgruppe, Serverbetriebssystemmaschine (nur bei Auswahl von Serverbetriebssystemmaschine in einer Bereitstellungsgruppe) und Bereich zur Verfügung. |
| Anzeigen der Nutzung gehosteter Anwendungen | Die Verfügbarkeit dieser Funktion hängt von den Lizenzen des Unternehmens ab.<br><br>Wählen Sie auf der Registerkarte "Kapazitätsverwaltung" die Registerkarte "Verwendung gehosteter Anwendungen" und dann die Bereitstellungsgruppe und den Zeitraum, um eine Kurve der höchsten gleichzeitigen Nutzung sowie eine Tabelle mit der anwendungsbasierten Verwendung anzuzeigen. In der Tabelle "Anwendungsbasierte Verwendung" können Sie eine bestimmte Anwendung auswählen, um Details und eine Liste der Benutzer anzuzeigen, die die Anwendung verwenden oder verwendet haben. |
| Anzeigen der Nutzung von | In der Ansicht "Trends" wird die Desktopbetriebssystemnutzung nach Site und |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Desktop- und Serverbetriebssystem | Bereitstellungsgruppe angezeigt. Bei Auswahl von "Site" wird die Nutzung nach Bereitstellungsgruppe angezeigt. Bei Auswahl von "Bereitstellungsgruppe" wird die Nutzung nach Benutzer angezeigt.<br><br>In der Ansicht "Trends" wird außerdem die Serverbetriebssystemnutzung nach Site, Bereitstellungsgruppe und Maschine angezeigt. Bei Auswahl von "Site" wird die Nutzung nach Bereitstellungsgruppe angezeigt. Bei Auswahl von "Bereitstellungsgruppe" wird die Nutzung nach Maschine und nach Benutzer angezeigt. Bei Auswahl von "Maschine" wird die Nutzung nach Benutzer angezeigt. |
| Nutzung virtueller Maschinen anzeigen | Wählen Sie auf der Registerkarte "Nutzung" die Option "Desktopbetriebssystemmaschinen" oder "Serverbetriebssystemmaschinen", um einen Überblick über die Nutzung der VMs in Echtzeit zu erhalten, sodass Sie den Kapazitätsbedarf der Site schnell einschätzen können.<br><br>Verfügbarkeit der Desktopbetriebssysteme: zeigt den aktuellen Zustand der Desktopbetriebssystemmaschinen (VDIs) nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an.<br><br>Verfügbarkeit der Serverbetriebssysteme: zeigt den aktuellen Zustand der Serverbetriebssystemmaschinen nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an. |
| Netzwerkanalysedaten mit HDX Insight anzeigen | Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen.<br><br>Überwachen Sie auf der Registerkarte "Netzwerk" die Netzwerkanalyse, die eine kontextbezogene Ansicht der Benutzer, Anwendungen und Desktops im Netzwerk bereitstellt. Director bietet mit diesem Feature eine erweiterte Analyse des ICA-Datenverkehrs in der Bereitstellung. |

Die Flag-Symbole auf dem Diagramm weisen auf wichtige Ereignisse oder Aktionen für diesen Zeitraum hin. Bewegen Sie den Mauszeiger über das Flag und klicken Sie, um Ereignisse und Aktionen aufzulisten.

Hinweis: Anmeldedaten für HDX-Verbindungen werden für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine
- Verhindern von Verbindungen mit Maschinen

## Überwachen von Hotfixes

Zum Anzeigen der auf einem bestimmten Maschinen-VDA (physisch oder VM) installierten Hotfixes wählen Sie die Ansicht Maschinendetails.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

## Steuern der Energiezustände von Benutzermaschinen

Steuern Sie den Zustand der in Director ausgewählten Maschinen mit den Optionen für die Energieverwaltung. Diese Optionen stehen für Desktopbetriebssystemmaschinen, aber möglicherweise nicht für Serverbetriebssystemmaschinen zur Verfügung.

Hinweis: Diese Funktionen stehen nicht für physische Maschinen zur Verfügung, die Remote-PC-Zugriff verwenden.

| Befehl | Funktion |
|---|---|
| **Neu starten** | Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten, bevor die VM neu gestartet wird. Wählen Sie diese Option beispielsweise für den Neustart von Maschinen, die in Director mit "Konnten nicht gestartet werden" ausgewiesen werden. |
| **Neustart erzwingen** | Die VM wird neu gestartet, ohne dass sie heruntergefahren wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers und erneutes Anschließen und Einschalten des Servers. |
| **Herunterfahren** | Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten. |
| **Herunterfahren erzwingen** | Die VM wird zwingend heruntergefahren, ohne dass das Verfahren zum Herunterfahren durchgeführt wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers. Es werden möglicherweise nicht immer alle ausgeführten Prozesse heruntergefahren, sodass bei diesem Verfahren die Gefahr von Datenverlust besteht. |
| **Suspend** | Die laufende VM wird im aktuellen Zustand angehalten und dieser Zustand wird in einer Datei im Standardspeicherrepository gespeichert. Diese Option ermöglicht das Herunterfahren der VM auf dem Hostserver und später, nach einem Neustart, die Wiederaufnahme der VM mit dem ursprünglichen Ausführungsstatus. |
| **Fortfahren** | Nimmt eine angehaltene VM wieder auf und stellt den ursprünglichen Ausführungsstatus wieder her. |
| **Starten** | Startet eine ausgeschaltete VM. |

Sollten die Energieverwaltungsaktionen fehlschlagen, zeigen Sie mit der Maus auf die Warnung und es wird eine Meldung mit Details zum Fehler angezeigt.

## Verhindern von Verbindungen mit Maschinen

Verwenden Sie den Wartungsmodus, um vorübergehend neue Verbindungen zu verhindern, während der entsprechende Administrator Wartungsaufgaben am Image durchführt.

Wenn Sie den Wartungsmodus auf Maschinen aktivieren, werden keine neuen Verbindungen zugelassen, bis Sie ihn wieder deaktivieren. Wenn Benutzer momentan angemeldet sind, wird der Wartungsmodus erst wirksam, sobald alle Benutzer abgemeldet sind. Benutzern, die sich nicht abmelden, müssen Sie eine Nachricht senden, die sie darüber informiert, dass die Maschine zu einem bestimmten Zeitpunkt heruntergefahren wird. Verwenden Sie die Energieverwaltung, um die Maschinen zwingend herunterzufahren.

1. Wählen Sie die Maschine aus, z. B. auf der Ansicht Benutzerdetails, oder eine Gruppe von Maschinen in der Ansicht Filter.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf Wartungsmodus und aktivieren Sie die Option.

Wenn ein Benutzer versucht, eine Verbindung zu einem zugewiesenen Desktop herzustellen, während er im Wartungsmodus ist, wird eine Meldung angezeigt, dass der Desktop zurzeit nicht verfügbar ist. Es können keine neuen Verbindungen hergestellt werden, bis der Wartungsmodus deaktiviert wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Warnungen und Benachrichtigungen

Jul 22, 2016

Dieser Abschnitt enthält folgende Themen:


Anzeigen von Warnungen

Erstellen von Warnungsrichtlinien

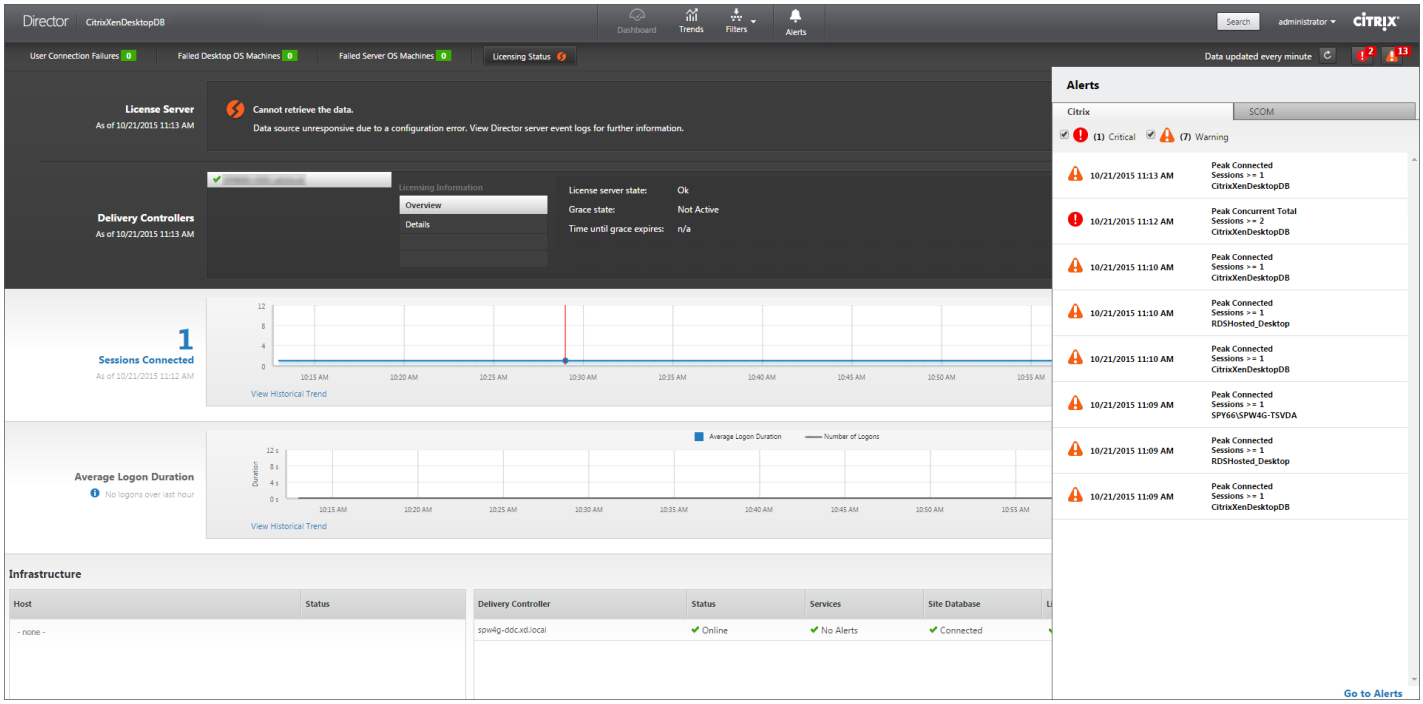
Bedingungen für Warnungsrichtlinien

SCOM-Warnungen

Konfigurieren der SCOM-Integration


## Anzeigen von Warnungen

In Director werden im Dashboard und in anderen Ansichten der oberen Ebene Warnungen und kritische Warnungen mit entsprechenden Symbolen angezeigt. Die Anzeige von Warnungen wird jede Minute automatisch aktualisiert und kann bei Bedarf auch manuell aktualisiert werden.



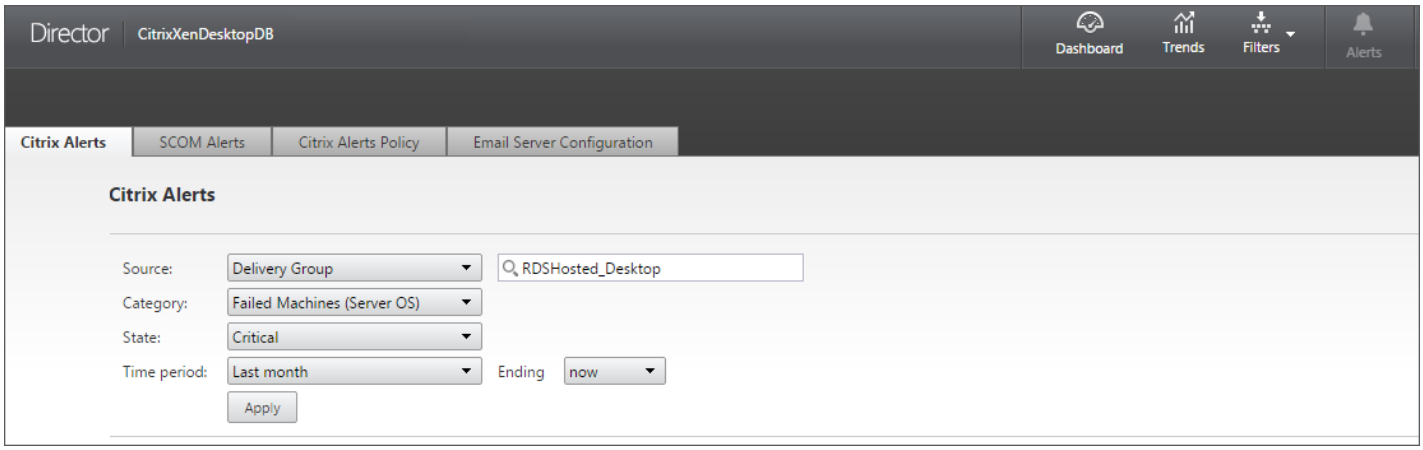

Eine Warnung (gelbes Dreieck) zeigt an, dass der minimale Schwellenwert einer Bedingung erreicht wurde.

Eine kritische Warnung (roter Kreis) zeigt an, dass der maximale Schwellenwert einer Bedingung überschritten wurde.

Detaillierte Informationen zu Warnungen können Sie aufrufen, indem Sie eine Warnung auf der Randleiste auswählen, auf den Link **Warnmeldungen** unten auf der Randleiste klicken oder oben auf der Director-Seite **Warnungen** wählen.

In der Ansicht "Warnungen" können Sie Warnungen filtern und exportieren. Beispielsweise können Sie fehlerhafte Serverbetriebssystemmaschinen für eine bestimmte Bereitstellungsgruppe im vergangenen Monat anzeigen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

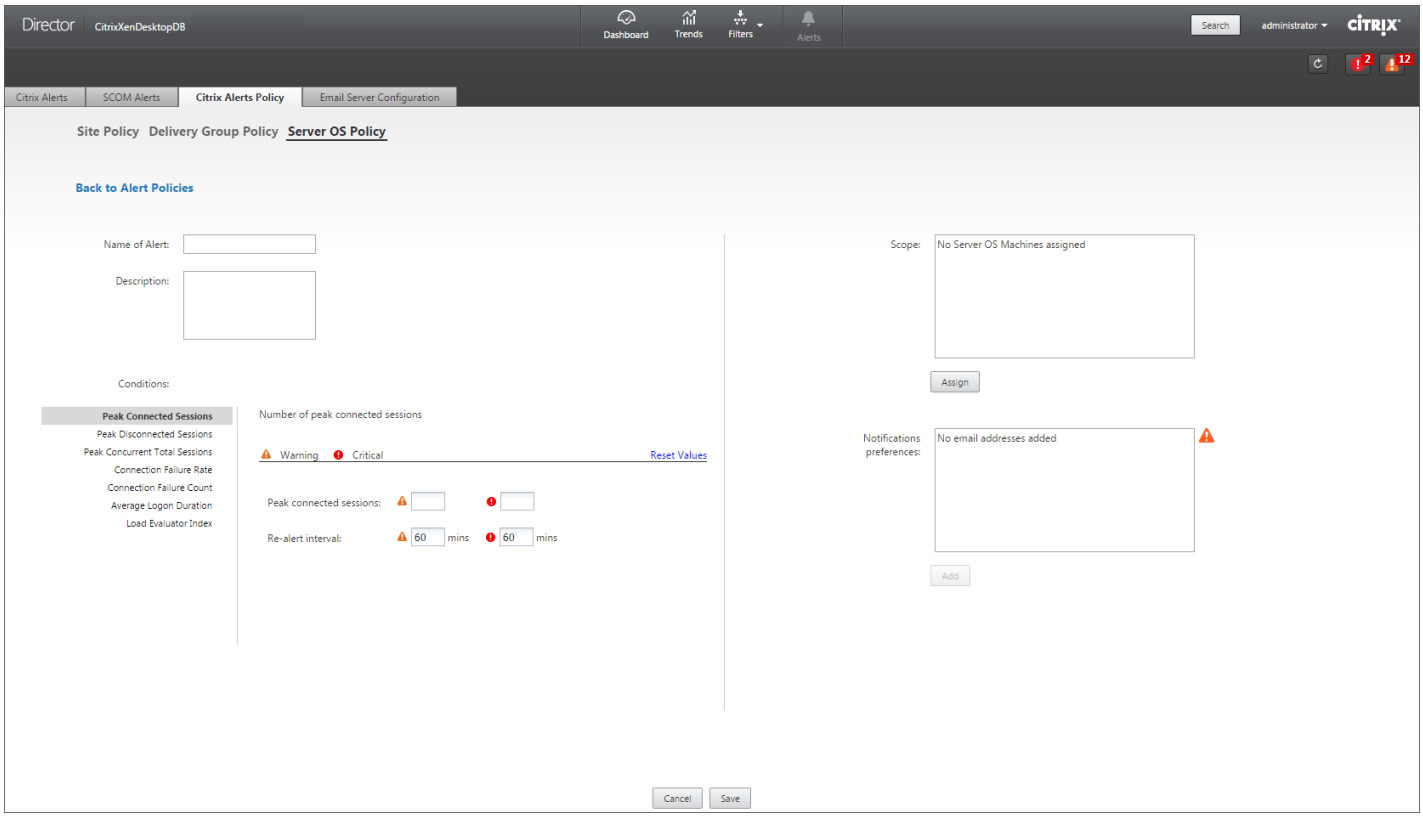



**Citrix Warnungen**: Citrix Warnungen in Director stammen von Citrix Komponenten. Sie können Citrix Warnungen in Director über **Warnungen** > **Citrix Warnungsrichtlinie** konfigurieren. Im Rahmen der Konfiguration können Sie den Versand von Benachrichtigungen per E-Mail an Personen und Gruppen festlegen, wenn die Schwellenwerte erreicht bzw. überschritten und Warnungen generiert werden. Weitere Informationen zum Einrichten von Citrix Warnungen finden Sie unter Erstellen von Warnungsrichtlinien.

**SCOM-Warnungen**: Warnungen von Microsoft System Center 2012 Operations Manager (SCOM) enthalten detaillierte Angaben zu Datencenterintegrität und Leistung in Director. Weitere Informationen finden Sie unter "SCOM-Warnungen" und "Konfigurieren der SCOM-Integration".

Die neben den Warnsymbolen vor dem Erweitern der Randleiste angezeigte Zahl entspricht der Summe der Citrix und SCOM-Warnungen.

## Erstellen von Warnungsrichtlinien





© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gehen Sie zum Erstellen einer Warnungsrichtlinie, z. B. zum Generieren einer Warnung bei Eintreten bestimmter Sitzungszahlbedingungen, folgendermaßen vor:

1. Navigieren Sie zu **Warnungen** > **Citrix Warnmeldungsrichtlinie** und wählen Sie beispielsweise "Serverbetriebssystemrichtlinie".
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein und legen Sie die Bedingungen zum Auslösen der Warnung fest. Geben Sie beispielsweise für die Kategorie "Warnung" und "Kritisch" Werte für "Max. verbundener Sitzungen", "Max. getrennter Sitzungen" und "Max. gleichzeitiger Sitzungen insgesamt" ein. Die Werte der Kategorie "Warnung" dürfen nicht größer sein als die der Kategorie "Kritisch". Weitere Informationen finden Sie unter "Bedingungen für Warnungsrichtlinien".
4. Legen Sie das Warnmeldungsintervall fest. Wenn die Bedingungen für die Warnung weiterhin erfüllt sind, wird die Warnung nach diesem Zeitintervall erneut ausgelöst und es wird, sofern dies in der Warnungsrichtlinie so festgelegt ist, eine E-Mail-Benachrichtigung generiert. Wird eine Warnung geschlossen, wird nach dem Warnmeldungsintervall keine E-Mail-Benachrichtigung generiert.
5. Legen Sie den Bereich fest. Wählen Sie beispielsweise eine Bereitstellungsgruppe.
6. Geben Sie in den Benachrichtigungseinstellungen an, wer per E-Mail benachrichtigt werden soll, wenn die Warnung ausgelöst wird. Zum Festlegen von E-Mail-Einstellungen für Warnungsrichtlinien müssen Sie auf der Registerkarte **E-Mail-Serverkonfiguration** einen E-Mail-SMTP-Server angeben.
7. Klicken Sie auf **Save**.

Wird eine Richtlinie mit einem Bereich von 20 oder mehr Bereitstellungsgruppen erstellt, kann der Abschluss der Konfiguration ca. eine halbe Minute dauern. Während dieses Zeitraums wird ein Drehfeld angezeigt.

Wenn Sie mehr als 50 Richtlinien pro Bereitstellungsgruppe für bis zu 20 eindeutige Bereitstellungsgruppen (insgesamt 1000 Bereitstellungsgruppenziele) erstellen, nimmt die Reaktionszeit u. U. um mehr als 5 Sekunden zu.

## Bedingungen für Warnungsrichtlinien

| **Bedingung der Warnungsrichtlinie** | **Beschreibung und empfohlene Aktionen** |
|---|---|
| Max. verbundener Sitzungen | Maximalzahl verbundener Sitzungen<br><br>Empfohlene Aktionen:<br><br>• Prüfen Sie die Maximalzahl verbundener Sitzungen in der Trendansicht von Director.<br>• Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.<br>• Fügen Sie neue Maschinen hinzu, falls erforderlich. |
| Max. getrennter Sitzungen | Maximalzahl getrennter Sitzungen<br><br>Empfohlene Aktionen:<br><br>• Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | • Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.<br>• Fügen Sie neue Maschinen hinzu, falls erforderlich.<br>• Melden Sie getrennte Sitzungen ab, falls erforderlich. |
| Max. gleichzeitiger Sitzungen insgesamt | Maximalzahl gleichzeitiger Sitzungen<br><br>Empfohlene Aktionen:<br><br>• Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director.<br>• Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist.<br>• Fügen Sie neue Maschinen hinzu, falls erforderlich.<br>• Melden Sie getrennte Sitzungen ab, falls erforderlich. |
| Verbindungsfehlerrate | Verbindungsfehler während der letzten Stunde in Prozent. Verhältnis der Summe aller Fehler zur Summe aller Verbindungsversuche.<br><br>• Überprüfen in Director die Ansicht "Fehlertrends" auf Ereignisse aus dem Konfigurationsprotokoll.<br>• Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind. |
| Anzahl Verbindungsfehler | Zahl der Verbindungsfehler während der letzten Stunde<br><br>Empfohlene Aktionen:<br><br>• Überprüfen in Director die Ansicht "Fehlertrends" auf Ereignisse aus dem Konfigurationsprotokoll.<br>• Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind. |
| Fehlerhafte Maschinen (Desktop-OS) | Zahl fehlerhafter Desktopbetriebssystemmaschinen<br><br>Empfohlene Aktionen:<br><br>• Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch. Weitere Informationen finden Sie unter "Behandeln von Benutzerproblemen". |
| Fehlerhafte Maschinen (Server-OS) | Zahl fehlerhafter Serverbetriebssystemmaschinen<br><br>Empfohlene Aktionen:<br><br>• Fehler können aus verschiedenen Gründen auftreten und |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch. |
| Durchschnittliche Anmeldedauer | Durchschnittliche Dauer der Anmeldungen in der letzten Stunde.<br><br>Empfohlene Aktionen:<br><br>• Überprüfen Sie die aktuellen Daten zur Anmeldedauer im Dashboard von Director. Melden sich viele Benutzer innerhalb kurzer Zeit an, kann die Anmeldung länger dauern.<br>• Überprüfen Sie Baseline und Aufschlüsselung der Anmeldungen zur Ursachenfindung.<br><br>Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen. |
| Lastauswertungsprogrammindex | Wert des Lastauswertungsprogrammindex der letzten 5 Minuten.<br><br>Empfohlene Aktionen:<br><br>• Prüfen Sie in Director auf Serverbetriebssystemmaschinen, die mit Spitzenlast ausgeführt werden.<br>• Zeigen Sie das Dashboard (Fehler) und die Trendansicht für den Lastauswertungsprogrammindex an. |

## SCOM-Warnungen

Wird Microsoft System Center 2012 Operations Manager in Director integriert, können Warnungen von SCOM im Dashboard und in anderen Ansichten der obersten Ebene in Director angezeigt werden.

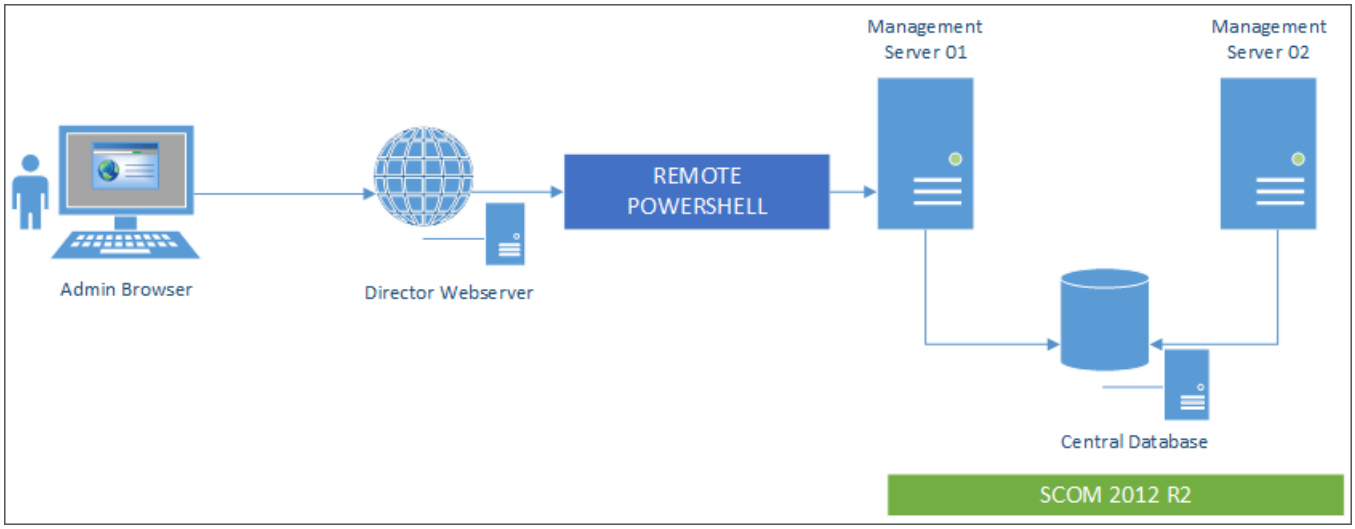
SCOM-Warnungen werden parallel mit Citrix Warnungen angezeigt. Sie können auf SCOM-Warnungen über die SCOM-Registerkarte auf der Randleiste zugreifen und Details anzeigen.

Sie können Warnungen eines Alters von bis zu einem Monat anzeigen, sortieren und filtern und die gefilterten Informationen in CSV-, Excel- und PDF-Berichte exportieren.

## Konfigurieren der SCOM-Integration

Bei einer SCOM-Integration werden Daten mit Remote-PowerShell 3.0 oder höher beim SCOM-Verwaltungsserver abgefragt und es besteht eine beständige Runspace-Verbindung in der Director-Sitzung des Benutzers. Director und der SCOM-Server müssen über dieselbe PowerShell-Version verfügen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




Anforderungen für die SCOM-Integration:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 oder höher (PowerShell-Versionen in Director und auf dem SCOM-Server müssen übereinstimmen)
- Quad-Core-CPU mit 16 GB RAM (empfohlen)
- Ein primärer Verwaltungsserver für SCOM muss in der web.config-Datei von Director konfiguriert werden. Dafür können Sie das Tool DirectorConfig verwenden.
- Citrix empfiehlt die Konfiguration des Director-Administratorkontos mit der SCOM-Rolle "Operator", damit die vollständigen Warnungsinformationen in Director abgerufen werden können. Ist das nicht möglich, kann mit dem DirectorConfig-Tool ein SCOM-Administratorkonto in der Datei web.config konfiguriert werden. Dies wird jedoch nicht empfohlen.
- Citrix empfiehlt, nicht mehr als 10 Director-Administratoren pro SCOM-Verwaltungsserver zu konfigurieren. Auf diese Weise wird der SCOM-Verwaltungsserver zur Gewährleistung der optimalen Leistung nur mäßig belastet.

Auf dem Director-Server

1. Geben Sie auf dem Director-Server **Enable-PSRemoting** ein, um das PowerShell-Remoting zu aktivieren.

2. Fügen Sie den SCOM-Verwaltungsserver der Liste "TrustedHosts" hinzu. Öffnen Sie eine PowerShell-Eingabeaufforderung mit erhöhten Rechten und führen Sie die folgenden Befehle aus:

   a. Abrufen der aktuellen TrustedHosts-Liste

command KOPIEREN

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

   b. Fügen Sie den SCOM-Verwaltungsserver der Liste "TrustedHosts" hinzu. steht für die von dem Cmdlet "Get-Item" zurückgegebenen vorhandenen Einträge.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```command
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

Konfigurieren von SCOM mit dem Tool DirectorConfig

```command
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

Auf dem SCOM-Verwaltungsserver

1. Weisen Sie einer SCOM-Administratorrolle Director-Administratoren zu.

   a. Öffnen Sie die SCOM-Verwaltungskonsole und navigieren Sie zu **Verwaltung** > **Sicherheit** > **Benutzerrollen**.

   b. Unter "Benutzerrollen" können Sie Benutzerrollen erstellen und bearbeiten. Es gibt vier Kategorien von SCOM-Operatoren. Über diese Rollen wird die Art des Zugriffs auf SCOM-Daten festgelegt. Ein Operator der Kategorie "Schreibgeschützt" kann beispielsweise den Verwaltungsbereich nicht sehen und keine Regeln, Maschinen und Konten erkennen oder verwalten. Eine SCOM-Operatorrolle entspricht einer vollständigen Administratorrolle.

   Hinweis:

   Ist einem Director-Administrator eine andere Rolle als "Operator" zugewiesen, kann er die nachfolgend aufgeführten Arbeitsschritte nicht ausführen.

      i. Sind mehrere Verwaltungsserver konfiguriert und fällt der primäre Server aus, kann der Director-Administrator keine Verbindung mit dem sekundären Verwaltungsserver herstellen.
      Der primäre Verwaltungsserver ist der in der Director-Datei web.config konfigurierte Server und mit dem oben in Schritt 3 im DirectorConfig-Tool angegebenen identisch. Die sekundären Verwaltungsserver stehen mit dem primären Verwaltungsserver in einer Peerbeziehung.

      ii. Beim Filtern von Warnungen kann der Director-Administrator die Warnungsquelle nicht suchen. Dies erfordert Operator-Berechtigung.

   c. Zum Ändern einer Benutzerrolle klicken Sie mit der rechten Maustaste auf die Rolle und dann auf "Eigenschaften".

   d. In dem Dialogfeld mit den Benutzerrolleneigenschaften können Sie Director-Administratoren zu der angegebenen Benutzerrolle hinzufügen oder aus dieser entfernen.

2. Fügen Sie der Benutzergruppe "Remoteverwaltung" auf dem SCOM-Verwaltungsserver Director-Administratoren hinzu. Dadurch können Director-Administratoren eine Remote-PowerShell-Verbindung herstellen.

3. Geben Sie **Enable-PSRemoting** ein, um PowerShell-Remoting zu aktivieren.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Legen Sie die Limits für die Eigenschaften der WS-Verwaltung fest:

a. Ändern von MaxConcurrentUsers:

Befehlszeilenschnittstelle (CLI):

```
command
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

PS:

```
command
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. Ändern von MaxShellsPerUser:

Befehlszeilenschnittstelle (CLI):

```
command
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

PS:

```
command
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. Ändern von MaxMemoryPerShellMB:

Befehlszeilenschnittstelle (CLI):

```
command
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

PS:

command KOPIEREN

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. Um sicherzustellen, dass die SCOM-Integration in Umgebungen mit gemischten Domänen funktioniert, legen Sie folgenden Registrierungseintrag fest:

Pfad: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Schlüssel: LocalAccountTokenFilterPolicy

Typ: DWord

Wert: 1

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Nach dem Einrichten der SCOM-Integration wird möglicherweise die Meldung "Die aktuellen SCOM-Warnmeldungen können nicht abgerufen werden" angezeigt. Suchen Sie in den Director-Serverereignisprotokollen weitere Informationen. Anhand der Informationen in den Serverereignisprotokollen können Sie das Problem identifizieren und beheben. Mögliche Ursachen:

- Unterbrechung der Netzwerkverbindung am Computer mit Director oder SCOM
- SCOM-Dienst nicht verfügbar oder überlastet
- Keine Autorisierung aufgrund einer Änderung an den Berechtigungen des Benutzers
- Fehler in Director beim Verarbeiten der SCOM-Daten
- Nicht übereinstimmende PowerShell-Version zwischen Director und SCOM-Server.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Delegierte Administration und Director

Jul 08, 2016

Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche. Berechtigungen richten sich nach der Administratorrolle und dem Geltungsbereich dieser Rolle. Beispiel: Einem Administrator wird die Helpdeskadministratorrolle zugewiesen, bei der der Geltungsbereich die Verantwortung für Endbenutzer an nur einer Site umfasst.

Weitere Informationen über das Erstellen von delegierten Administratoren finden Sie unter Delegierte Administration.

Durch die administrativen Berechtigungen wird festgelegt, wie die Director-Benutzeroberfläche für Administratoren dargestellt wird und welche Aufgaben sie ausführen können. Mit Berechtigungen wird Folgendes festgelegt:

- Die Seiten, auf die der Administrator zugreifen kann, kollektiv als "Ansicht" bezeichnet
- Die Desktops, Maschinen und Sitzungen, die der Administrator anzeigen und verwenden kann
- Die Befehle, die der Administrator ausführen kann, z. B. das Spiegeln einer Benutzersitzung oder das Aktivieren des Wartungsmodus

Über die integrierten Rollen und Berechtigungen wird außerdem gesteuert, wie Administratoren Director verwenden:

| **Administratorrolle** | **Berechtigungen in Director** |
|---|---|
| Volladministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Bereitstellungsgruppenadministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Lesezugriffadministrator | Kann auf alle Ansichten zugreifen und alle Objekte in angegebenen Geltungsbereichen sowie globale Informationen anzeigen. Kann Berichte aus HDX-Kanälen herunterladen und Trenddaten mit der Exportoption in der Ansicht "Trends" exportieren.<br>Kann keine anderen Befehle ausführen oder Daten in den Ansichten ändern. |
| Helpdeskadministrator | Kann nur auf die Ansichten "Helpdesk" und "Benutzerdetails" zugreifen und nur Objekte anzeigen, die dem Administrator zur Verwaltung übertragen wurden. Kann eine Benutzersitzung spiegeln und Befehle für diesen Benutzer ausführen. Kann Vorgänge im Wartungsmodus ausführen. Kann Energieoptionen auf Desktopbetriebssystemmaschinen verwenden.<br>Kann nicht auf das Dashboard, Trends, Warnungen oder Filteransichten zugreifen. Kann keine Energieoptionen auf Serverbetriebssystemmaschinen verwenden. |
| Maschinenkatalogadministrator | Kein Zugriff. Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen. Dieser Benutzer kann auf die Seite "Maschinendetails" zugreifen (maschinenbasierte Suche). |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Administratorrolle | Berechtigungen in Director |
| --- | --- |
| Hostadministrator | Kein Zugriff: Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen. |

**Konfigurieren von benutzerdefinierten Rollen für Director-Administratoren**

In Studio können Sie auch Director-spezifische benutzerdefinierte Rollen konfigurieren, die den Anforderungen Ihrer Organisation besser gerecht werden und eine flexiblere Delegierung von Berechtigungen ermöglichen. Sie können beispielsweise die integrierte Helpdeskadministratorrolle einschränken, sodass dieser Administrator keine Sitzungen abmelden kann.

Wenn Sie eine benutzerdefinierte Rolle mit Director-Berechtigungen erstellen, müssen Sie dieser auch andere allgemeine Berechtigungen erteilen:

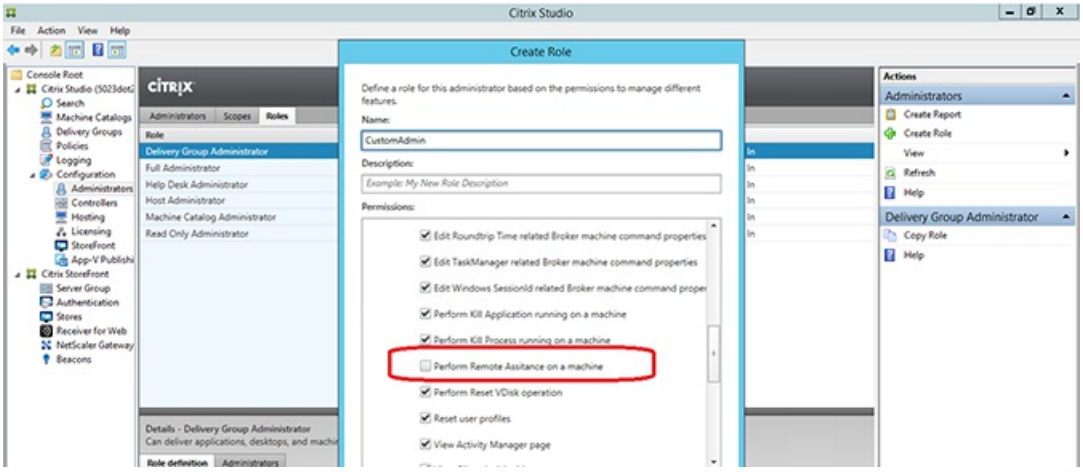
- Delivery Controller-Berechtigung zur Anmeldung bei Director.
- Berechtigungen für Bereitstellungsgruppen zum Anzeigen der zu diesen gehörigen Daten in Director.

Alternativ können Sie eine benutzerdefinierte Rolle erstellen, indem Sie eine vorhandene Rolle kopieren und dieser zusätzliche Berechtigungen für die verschiedenen Ansichten erteilen. Sie können beispielsweise die Rolle "Helpdesk" kopieren und Berechtigungen zum Anzeigen des Dashboards oder der Seiten "Filter" hinzufügen.

Wählen Sie die Director-Berechtigungen für die benutzerdefinierte Rolle, die Folgendes enthält:

- Abbrechen von auf Maschine ausgeführter Anwendung erzwingen
- Abbrechen von auf Maschine ausgeführtem Prozess erzwingen
- Remoteunterstützung für Maschine ausführen
- Vorgang zum Zurücksetzen von vDisk ausführen
- Benutzerprofile zurücksetzen
- Anzeigen der Seite "Clientdetails"
- Anzeigen der Seite "Dashboard"
- Anzeigen der Seite "Filter"
- Anzeigen der Seite "Maschinendetails"
- Anzeigen der Seite "Trends"
- Anzeigen der Seite "Benutzerdetails"

In diesem Beispiel ist das Spiegeln (Remoteunterstützung für Maschine ausführen) deaktiviert.




Aus der Liste der Berechtigungen für andere Komponenten sollten Sie zusätzlich folgende Berechtigungen berücksichtigen:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Bereitstellungsgruppen:
  - Aktivieren/Deaktivieren des Wartungsmodus einer Maschine mit der Bereitstellungsgruppenmitgliedschaft
  - Ausführen von Energievorgängen auf Windows-Desktopmaschinen mit der Bereitstellungsgruppenmitgliedschaft
  - Ausführen der Sitzungsverwaltung auf Maschinen unter mit der Bereitstellungsgruppenmitgliedschaft


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Sichere Bereitstellung von Director

Jul 08, 2016

In diesem Artikel werden Bereiche behandelt, die sich bei der Bereitstellung und Konfiguration von Director auf die Systemsicherheit auswirken können.

## Konfigurieren von Microsoft Internetinformationsdienste (IIS)

Sie können Director mit einer eingeschränkten IIS-Konfiguration konfigurieren. Dies ist jedoch nicht die IIS-Standardkonfiguration.

**Dateinamenerweiterungen**

Sie können nicht aufgeführte Dateinamenerweiterungen ausschließen.

Director benötigt die Dateinamenerweiterungen bei der Anforderungsfilterung:

- .aspx
- .css
- .html
- .js
- .png

Director benötigt die folgenden HTTP-Verben bei der Anforderungsfilterung. Sie können nicht aufgeführte Verben ausschließen.

- GET
- POST
- HEAD

Director erfordert Folgendes nicht:

- ISAPI-Filter
- ISAPI-Erweiterungen
- CGI-Programme
- FastCGI-Programme

> **Important**
>
> - Director erfordert volles Vertrauen. Legen Sie jedoch nicht die globale .NET-Vertrauensebene auf "Hoch" oder niedriger fest.
> - Director unterhält einen separaten Anwendungspool. Um die Director-Einstellungen zu ändern, wählen Sie die Director-Site und führen Sie die Änderungen durch.

## Konfigurieren von Benutzerrechten

Wenn Director installiert wird, werden den Anwendungspools die Anmeldeberechtigung "Anmelden als Dienst" und die Privilegien "Anpassen von Speicherkontingenten für einen Prozess", "Generieren von Sicherheitsüberwachungen" und "Ersetzen eines Tokens auf Prozessebene" zugewiesen. Dies ist normales Installationsverhalten beim Erstellen von


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Anwendungspools.

Sie brauchen die Benutzerrechte nicht zu ändern. Diese Privilegien werden von Director nicht verwendet und werden automatisch deaktiviert.

Zertifikate in Director:

- Zur Verwendung von HTTPS können vertrauenswürdige Zertifikate konfiguriert und verwendet werden.

## Kommunikation mit Director

Citrix empfiehlt für Produktionsumgebungen die Verwendung von IPsec (Internet Protocol Security) oder von HTTPS-Protokollen zum Schutz der Datenübertragung zwischen Director und Ihren Servern. IPsec bietet eine Reihe von Standarderweiterungen des Internetprotokolls, die authentifizierte und verschlüsselte Kommunikation mit Datenintegrität und Schutz vor Wiedergabeangriffen bieten. Da IPsec ein Protokollsatz der Vermittlungsschicht ist, können Protokolle höherer Stufen es unverändert verwenden. HTTPS verwendet Secure Sockets Layer (SSL) und Transport Layer Security (TLS) für eine starke Datenverschlüsselung.

TLS-Relay kann verwendet werden, um den Datenverkehr zwischen Director und XenApp-/XenDesktop-Servern zu schützen. Weitere Informationen finden Sie in folgendem Blogbeitrag: Securing Citrix Director: OData Interface through TLS.

Citrix empfiehlt, die Kommunikation zwischen Director und Benutzergeräten mit NetScaler Gateway und HTTPS zu schützen. Damit HTTPS verwendet werden kann, muss die Microsoft Internet Information Services (IIS)-Instanz, auf der der Authentifizierungsdienst gehostet wird, für HTTPS konfiguriert sein. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet Director HTTP für die Kommunikation. Citrix empfiehlt dringend, keine ungeschützten Benutzerverbindungen mit Director in einer Produktionsumgebung zu aktivieren.

## Isolierung der Director-Sicherheit

Falls Sie Webanwendungen in derselben Webdomäne (Domänenname und Port) wie Director bereitstellen, können die mit diesen Webanwendungen verbundenen Sicherheitsrisiken eventuell auch die Sicherheit der Director-Bereitstellung negativ beeinflussen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von Director in einer getrennten Webdomäne.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7

Jul 08, 2016

Wenn Benutzer auf ihren Geräten VDAs einer Version vor XenDesktop 7 installiert haben, ergänzt Director Informationen aus der Bereitstellung durch Echtzeitstatus und -metrik über Windows-Remoteverwaltung (WinRM).

Darüber hinaus können Sie mit dem hier beschriebenen Verfahren WinRM für die Verwendung mit Remote PC in XenDesktop 5.6 Feature Pack1 konfigurieren.

Standardmäßig verfügen nur lokale Administratoren des Desktopcomputers (in der Regel Domänenadministratoren und andere privilegierte Benutzer) über die Berechtigungen, die zum Anzeigen der Echtzeitdaten erforderlich sind.

Informationen zum Installieren und Konfigurieren von WinRM finden Sie unter CTX125243.

Um anderen Benutzern das Anzeigen von Echtzeitdaten zu ermöglichen, müssen Sie diesen Berechtigungen erteilen. Beispiel: Angenommen, es gibt mehrere Director-Benutzer (HelpDeskUserA, HelpDeskUserB usw.), die zu einer Active Directory-Sicherheitsgruppe namens "HelpDeskUsers" gehören. Der Gruppe wurde in Studio die Helpdeskadministratorrolle mit den erforderlichen Delivery Controller-Berechtigungen zugewiesen. Die Gruppe benötigt jedoch auch Zugriff auf Informationen vom Desktopcomputer.

Sie haben zwei Möglichkeiten, die Berechtigungen für den erforderlichen Zugriff zu konfigurieren:

- Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)
- Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)

**Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)**

Director verwendet standardmäßig ein Identitätswechselmodell: Die WinRM-Verbindung mit der Desktopmaschine wird mit der Identität des Director-Benutzers hergestellt. Aus diesem Grund muss der Benutzer über die erforderlichen Berechtigungen auf dem Desktop verfügen.

Sie können diese Berechtigungen mit einer der folgenden beiden Methoden konfigurieren (nachfolgend beschrieben):

1. Hinzufügen von Benutzern zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen der von Director benötigten spezifischen Berechtigungen für Benutzer. Bei dieser Option wird vermieden, dass Director-Benutzer (beispielsweise die HelpDeskUsers-Gruppe) Volladministratorrechte auf der Maschine erhalten.

**Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)**

Anstatt den Director-Benutzern Berechtigungen für die Desktopmaschinen zu erteilen, können Sie Director so konfigurieren, dass WinRM-Verbindungen mit einer Dienstidentität hergestellt werden, und ausschließlich dieser Dienstidentität die entsprechenden Berechtigungen erteilen.

Bei diesem Modell sind die Benutzer von Director nicht berechtigt, selbst WinRM-Aufrufe zu tätigen. Sie können nur mit Director auf die Daten zugreifen.

Der Director-Anwendungspool in IIS ist für die Ausführung als Dienstidentität konfiguriert. Dies ist standardmäßig das virtuelle Konto "APPPOOL\Director". Beim Herstellen von Remoteverbindungen wird dieses Konto als das Active Directory-Computerkonto des Servers angezeigt, z. B. MyDomain\DirectorServer$. Sie müssen dieses Konto mit den entsprechenden


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Berechtigungen konfigurieren.

Wenn mehrere Director-Websites bereitgestellt werden, müssen Sie das Computerkonto jedes Webservers in eine Active Directory-Sicherheitsgruppe setzen, die entsprechende Berechtigungen hat.

Um Director so einzustellen, dass anstelle der Benutzeridentität die Dienstidentität für WinRM verwendet wird, konfigurieren Sie die folgende Einstellung, wie unter Erweiterte Konfiguration beschrieben:

Service.Connector.WinRM.Identity = Service
Sie haben zwei Möglichkeiten, diese Berechtigungen zu konfigurieren:

1. Hinzufügen des Dienstkontos zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen Sie dem Dienstkonto die für Director erforderlichen Berechtigungen (siehe weiter unten). So kann eine Erteilung von Volladministratorrechten für das Dienstkonto auf der Maschine vermieden werden.

**Zuweisen von Berechtigungen für einen bestimmten Benutzer oder eine bestimmte Gruppe**

Die folgenden Berechtigungen sind erforderlich, damit Director auf die von der Desktopmaschine benötigten Informationen über WinRM zugreifen kann:

- Lese- und Ausführberechtigungen in WinRM RootSDDL
- WMI-Namespace-Berechtigungen:
  - root/cimv2 – Remotezugriff
  - root/citrix – Remotezugriff
  - root/RSOP – Remotezugriff und Ausführen
- Zugehörigkeit zu diesen lokalen Gruppen:
  - Systemmonitorbenutzer
  - Ereignisprotokollleser

Das ConfigRemoteMgmt.exe-Tool, das zum automatischen Erteilen dieser Berechtigungen verwendet wird, befindet sich auf dem Installationsmedium in den Ordnern x86\Virtual Desktop Agent und x64\Virtual Desktop Agent und auf dem Installationsmedium im Ordner "tools". Sie müssen allen Director-Benutzern Berechtigungen erteilen.

Um einer Active Directory-Sicherheitsgruppe, einem Benutzer oder einem Computerkonto Berechtigungen zu erteilen, oder um Aktionen auszuführen wie "Anwendung beenden und "Prozess beenden", führen Sie das Tool mit Administratorrechten an einer Eingabeaufforderung mit den folgenden Argumenten aus:

ConfigRemoteMgmt.exe /configwinrmuser domain\name
wobei name eine Sicherheitsgruppe, ein Benutzer oder ein Computerkonto ist.

Erteilen der erforderlichen Berechtigungen für eine Benutzersicherheitsgruppe:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
Erteilen von Berechtigungen für ein bestimmtes Computerkonto:

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
Für die Aktionen "Prozess beenden", "Anwendung beenden" und "Spiegeln":

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
Erteilen von Berechtigungen für eine Benutzergruppe:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all

 © 1999-2017 Citrix Systems, Inc. All rights reserved. 

Anzeigen der Hilfe für das Tool:

ConfigRemoteMgmt.exe


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Konfigurieren von HDX Insight

Jul 08, 2016

Hinweis: Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen.

HDX Insight ist die Integration der Netzwerkanalyse und der Leistungsverwaltung in Director:

- Die Netzwerkanalyse nutzt HDX Insight und stellt eine kontextbezogene Ansicht der Anwendungen und Desktops im Netzwerk bereit. Mit diesem Feature bietet Director eine erweiterte Analyse des ICA-Datenverkehrs in der Bereitstellung.
- Die Leistungsverwaltung bietet eine Verlaufsspeicherung und Trendberichte. Anhand der Beibehaltung historischer Daten können Sie im Gegensatz zur Echtzeitbewertung Trendberichte über Kapazität und Integrität usw. erstellen.

Nachdem Sie dieses Feature in Director aktivieren, liefert HDX Insight zusätzliche Informationen an Director:

- Auf der Seite Trends werden bereitstellungsübergreifend Auswirkungen auf Latenz und Bandbreite für Anwendungen, Desktops und Benutzer angezeigt.
- Auf der Seite Benutzerdetails werden Latenz- und Bandbreiteninformationen zu spezifischen Benutzersitzungen angezeigt.

**Einschränkungen**

- Die Roundtripzeitdaten für die ICA-Sitzung werden in Receiver für Windows 3.4 oder höher und Receiver für Mac 11.8 oder höher richtig angezeigt. Bei früheren Versionen von Receiver werden die Daten nicht richtig angezeigt.
- In der Trendansicht werden Anmeldedaten für HDX-Verbindungen für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.

**Konfigurieren der Netzwerkanalyse in Director**

Director bietet eine Netzwerkanalyse unter Nutzung von NetScaler HDX Insight, anhand derer Administratoren der Citrix Anwendungen und Desktops Probleme behandeln und korrelieren können, die auf eine schlechte Netzwerkleistung zurückzuführen sind.

NetScaler Insight Center muss in Director installiert und konfiguriert sein, damit die Netzwerkanalyse aktiviert werden kann. Insight Center ist eine virtuelle Maschine (Gerät), die von Citrix.com heruntergeladen wird. Mit der Netzwerkanalyse sammelt Director Daten zur Bereitstellung. Diese Informationen werden aus HDX Insight verwendet, das eine stabile Analyse des Citrix ICA-Protokolls zwischen dem Client und der Citrix Back-End-Infrastruktur bietet.

1. Suchen Sie auf dem Server, auf dem Director installiert ist, das Befehlszeilentool DirectorConfig in C:\inetpub\wwwroot\Director\tools und führen Sie es mit dem Parameter /confignetscaler an der Eingabeaufforderung aus.
2. Wenn Sie dazu aufgefordert werden, konfigurieren Sie den Maschinennamen (FQDN oder IP-Adresse) für NetScaler Insight Center sowie den Benutzernamen, das Kennwort und den HTTP- oder HTTPS-Verbindungstyp.
3. Melden Sie sich zum Prüfen der Änderungen ab und wieder an.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Behandeln von Benutzerproblemen

Jul 08, 2016

In der Ansicht **Helpdesk** (Seite **Aktivitäts-Manager**) in Director zeigen Sie Informationen über den Benutzer an:

- Überprüfen Sie die Details zur Anmeldung des Benutzers, zur Verbindung und zu den Anwendungen.
- Spiegeln Sie die Maschine des Benutzers.
- Behandeln Sie das Problem mit den in der folgenden Tabelle empfohlenen Aktionen und eskalieren Sie das Problem ggf. an den entsprechenden Administrator.

### Tipps zur Problembehandlung

| Problem des Benutzers | Lösungsvorschläge: |
|---|---|
| Anmeldung dauert lange oder schlägt periodisch oder wiederholt fehl | Diagnose von Benutzeranmeldeproblemen |
| Anwendung ist langsam oder reagiert nicht mehr | Beheben von Anwendungsfehlern |
| Verbindung ist fehlgeschlagen | Wiederherstellen von Desktopverbindungen |
| Sitzung ist langsam oder reagiert nicht | Wiederherstellen von Sitzungen |
| Video ist langsam oder von schlechter Qualität | Ausführen von Systemberichten für HDX-Kanäle |

Hinweis: Um sicherzustellen, dass der Computer nicht im Wartungsmodus ist, überprüfen Sie in der Ansicht Benutzerdetails den Bereich Maschinendetails.

### Suchtipps

Wenn Sie den Namen des Benutzers im Suchfeld eingeben, sucht Director in Active Directory nach Benutzern in allen Sites, die für Director konfiguriert wurden.

Wenn Sie den Namen einer Maschine, die von mehreren Benutzern verwendet wird, in ein Suchfeld eingeben, zeigt Director die Maschinendetails für die angegebene Maschine an.

Wenn Sie einen Endpunktnamen in ein Suchfeld eingeben, verwendet Director die nicht authentifizierten (anonymen) und die authentifizierten Sitzungen, die mit einem bestimmten Endpunkt verbunden sind, sodass Probleme in nicht authentifizierten Sitzungen behandelt werden können. Stellen Sie sicher, dass Endpunktnamen eindeutig sind, damit die Problembehandlung von nicht authentifizierten Sitzungen durchgeführt werden kann.

Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.
- Teileinträge ergeben eine Liste möglicher Übereinstimmungen.
- Nachdem Sie einige Buchstaben eines zweiteiligen Namens (Benutzername, Nachname und Vorname oder Anzeigename)

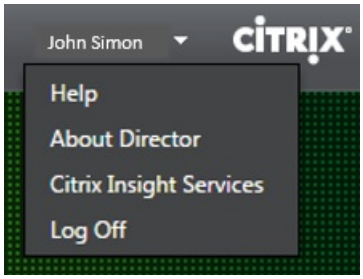

© 1999-2017 Citrix Systems, Inc. All rights reserved.

durch Leerzeichen getrennt eingegeben haben, enthalten die Ergebnisse Übereinstimmungen für beide Zeichenfolgen. Wenn Sie beispielsweisejo robeingeben, werden Zeichenfolgen wie "John Robertson" oder "Robert, Jones" als Ergebnisse angezeigt.

Klicken Sie auf das Director-Logo, um zur Startseite zurückzukehren.

### Zugriff auf Citrix Insight Services

Für zusätzliche Diagnoseinformationen können Sie über die Dropdownliste "Benutzer" in Director auf Citrix Insight Services (CIS) zugreifen. Die Informationen in CIS stammen aus mehreren Quellen einschließlich Call Home und Citrix Scout.




### Hochladen von Problembehandlungsinformationen zum technischen Support von Citrix

Führen Sie Citrix Scout auf einem Delivery Controller oder VDA aus, um wichtige Datenpunkte und CDF-Traces (Citrix Diagnosis Facility) für die Fehlerbehebung auf ausgewählten Computern zu erfassen. Mit Scout können Sie Daten sicher an Citrix Insight Services (CIS) hochladen, um den technischen Support von Citrix bei der Problembehandlung zu unterstützen. Der technische Support von Citrix nutzt die CIS-Plattform, um von Kunden gemeldete Probleme schneller zu lösen.

Scout wird mit XenApp- bzw. XenDesktop-Komponenten installiert. Je nach Windows-Version erscheint Scout im Startmenü bzw. Startbildschirm nach der Installation von (bzw. einem Upgrade auf) XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 oder XenApp 7.7.

Zum Starten von Scout über das Startmenü oder den Startbildschirm wählen Sie Citrix > Citrix Scout.

Informationen zum Verwenden und Konfigurieren von Scout und FAQ finden Sie unter CTX130147.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Spiegeln von Benutzern

Jul 08, 2016

Mit dem Feature Benutzer spiegeln in Director können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und damit arbeiten. Der Benutzer muss mit der zu spiegelnden Maschine verbunden sein. Wenn der Benutzer verbunden ist, wird der Name der verbundenen Maschine in der Titelleiste des Benutzers angezeigt.

1. Wählen Sie in der Ansicht Details die Benutzersitzung aus.
2. Aktivieren Sie die Spiegelung für die ausgewählte Benutzersitzung:
   - Klicken Sie zur Maschinenüberwachung in der Ansicht Aktivitäts-Manager auf Spiegeln.
   - Klicken Sie zur Sitzungsüberwachung in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Spiegeln.
3. Nach Initialisierung der Verbindung werden Sie in einem Dialogfeld aufgefordert, die Datei .msrcincident zu öffnen oder zu speichern.
4. Öffnen Sie die Vorfalldatei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
5. Weisen Sie die Benutzer an, auf Ja zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.

Fordern Sie den Benutzer auf, die Tastatur- und Maussteuerung freizugeben, damit Sie die Steuerung übernehmen können.

Richten Sie den Microsoft Internet Explorer-Browser so ein, dass die heruntergeladene Datei zur Microsoft-Remoteunterstützung (.msra) automatisch mit dem Remoteunterstützungsclient geöffnet wird.

Hierzu müssen Sie die Einstellung Automatische Eingabeaufforderung für Dateidownloads im Gruppenrichtlinien-Editor aktivieren:

Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Internetsystemsteuerung > Sicherheitsseite > Internetzone > Automatische Eingabeaufforderung für Dateidownloads.

Diese Option ist standardmäßig für Sites in der lokalen Intranetzone aktiviert. Wenn die Director-Site nicht zur lokalen Intranetzone gehört, sollten Sie die Site manuell dieser Zone hinzufügen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Senden von Nachrichten an Benutzer

Jul 08, 2016

Sie können über Director eine Nachricht an einen Benutzer senden, der mit einer oder mehreren Maschinen verbunden ist. Sie können beispielsweise mit dieser Funktion sofortige Benachrichtigungen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und die Rücksetzung von Profilen.

1. Wählen Sie in der Ansicht Aktivitäts-Manager den Benutzer aus und klicken Sie auf Details.
2. Klicken in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Nachricht senden.
3. Füllen Sie die Felder Betreff und Nachricht aus und klicken Sie auf Senden.

Wenn die Nachricht gesendet wird, wird in Director eine Bestätigungsmeldung angezeigt. Wenn die Maschine des Benutzers verbunden ist, wird dort eine entsprechende Nachricht angezeigt.

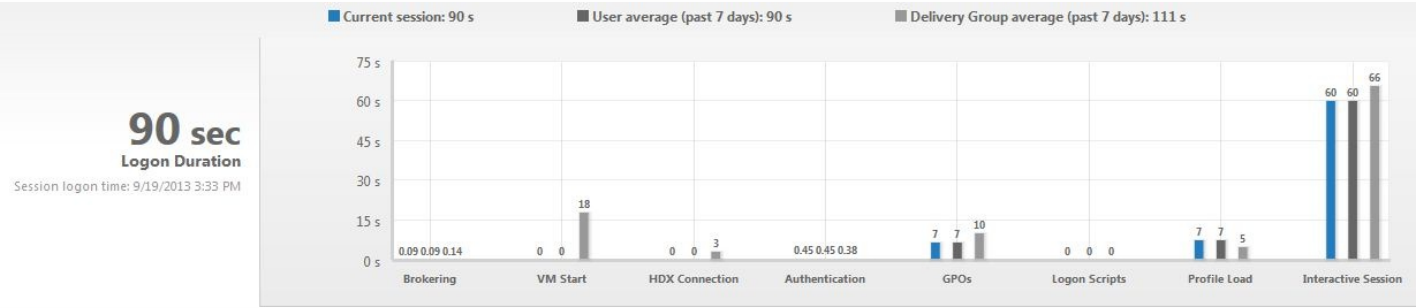
Wenn die Nachricht nicht gesendet wird, wird in Director eine Fehlermeldung angezeigt. Gehen Sie bei der Problembehandlung gemäß der Anweisungen in der Fehlermeldung vor. Geben Sie abschließend den Betreff und Text der Nachricht erneut ein und klicken Sie auf Noch einmal versuchen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Diagnose von Benutzeranmeldeproblemen

Jul 11, 2016

Mit den Anmeldedauerdaten können Sie Benutzeranmeldeprobleme beheben. In der Ansicht "Benutzerdetails" wird die Dauer als Zahlenwert angezeigt. Darunter sehen Sie den Zeitpunkt der Anmeldung und ein Diagramm mit den Phasen des Anmeldeprozesses.




Bereich "Anmeldedauer" in der Ansicht "Benutzerdetails"

Wenn Benutzer sich an XenApp und XenDesktop anmelden, werden die Phasen des Anmeldeprozesses vom Überwachungsdienst verfolgt, und zwar ab dem Zeitpunkt, wenn der Benutzer von Citrix Receiver aus eine Verbindung herstellt, bis zu dem Zeitpunkt, wenn der Desktop für die Verwendung bereit ist. Der große Wert auf der linken Seite ist die Gesamtanmeldedauer. Sie ergibt sich aus der Zeit, die zum Herstellen der Verbindung und Bereitstellen eines Desktops durch den Delivery Controller benötigt wird, plus der Zeit, die die Authentifizierung und Anmeldung an einem virtuellen Desktop erfordert. Die Dauer wird in Sekunden (oder Sekundenbruchteilen) in der lokalen Zeit im Webbrowser des Administrators angezeigt.

Mit den folgenden allgemeinen Schritten beheben Sie Benutzeranmeldeprobleme:

1. Überprüfen Sie in der Ansicht **Benutzerdetails** im Bereich "Anmeldedauer", welcher Anmeldezustand vorliegt.
   - Wenn Benutzer sich anmelden, wird der Anmeldeprozess in der Ansicht widergespiegelt.
   - Wenn der Benutzer angemeldet ist, wird im Bereich "Anmeldedauer" angezeigt, wie viel Zeit für die Anmeldung des Benutzers an der aktuellen Sitzung benötigt wurde.
2. Überprüfen Sie die Phasen des Anmeldeprozesses.

| Phase des Anmeldeprozesses | Beschreibung |
|---|---|
| Vermittlung | Zur Zuweisung des Desktops zum Benutzer benötigte Zeit. |
| VM-Start | Zum Starten einer virtuellen Maschine benötigte Zeit, wenn eine Sitzung den Start einer Maschine erforderte. |
| HDX-Verbindung | Zum Einrichten der HDX-Verbindung vom Client zur virtuellen Maschine benötigte Zeit. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Authentifizierung | Zum Abschließen der Authentifizierung bei der Remotesitzung benötigte Zeit. |
| Gruppenrichtlinienobjekte | Zum Anwenden von Gruppenrichtlinienobjekten benötigte Zeit, wenn Gruppenrichtlinieneinstellungen auf den virtuellen Maschinen aktiviert sind. |
| Anmeldeskripts | Zum Ausführen von Anmeldeskripts benötigte Zeit, wenn Anmeldeskripts für die Sitzung konfiguriert sind. |
| Profilladezeit | Zum Laden des Profils benötigte Zeit, wenn für den Benutzer Profileinstellungen auf der virtuellen Maschine konfiguriert sind. |
| Interaktive Sitzung | Zum Übergeben von Tastatur- und Maussteuerung an den Benutzer benötigte Zeit, nachdem das Profil geladen wurde. Dies dauert normalerweise am längsten von allen Phasen des Anmeldeprozesses und wird wie folgt berechnet:<br><br>Dauer der interaktiven Sitzung = Zeitstempel des Ereignisses "Desktop bereit" (Ereignis-ID 1000 auf VDA) - Zeitstempel des Ereignisses "Profilladezeit" (Ereignis-ID 2 auf VDA) |

Die Gesamtanmeldedauer ist keine genaue Summe der einzelnen Phasen. Beispiel: Einige Phasen treten parallel auf und in anderen Phasen wird eine zusätzliche Verarbeitung durchgeführt, die zu einer längeren Anmeldedauer als die Summe der einzelnen Phasen führen kann.

> **Hinweis**
>
> Im Anmeldedauerdiagramm werden die Anmeldephasen in Sekunden angezeigt. Zeitwerte unter einer Sekunde werden als Sekundenbruchteile angezeigt. Werte, die größer sind als eine Sekunde, werden auf die nächste halbe Sekunde aufgerundet. Aufgrund des Diagrammdesigns kann ein Höchstwert von 200 Sekunden auf der Y-Achse angezeigt werden. Bei Werten über 200 Sekunden wird der tatsächliche Wert über dem Balken angezeigt.

Um ungewöhnliche oder unerwartete Werte im Diagramm zu finden, vergleichen Sie die in jeder Phase der aktuellen Sitzung benötigte Zeit mit der durchschnittlichen Dauer für diesen Benutzer in den letzten sieben Tagen sowie mit der durchschnittlichen Dauer in den letzten sieben Tagen für alle Benutzer diese Bereitstellungsgruppe.

Eskalieren Sie wie erforderlich. Beispiel: Wenn der VM-Start langsam ist, liegt das Problem möglicherweise am Hypervisor, Sie können das Problem also an den Hypervisoradministrator eskalieren. Wenn die Vermittlungsdauer zu lang ist, können Sie das


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problem dem Siteadministrator melden, damit der Lastausgleich auf dem Delivery Controller überprüft wird.

Überprüfen Sie ungewöhnliche Unterschiede, u. a.:

- Fehlende (aktuelle) Anmeldeleisten
- Große Abweichung zwischen der aktuellen und der durchschnittlichen Dauer für diesen Benutzer. Mögliche Ursachen:
  - Es wurde eine neue Anwendung installiert.
  - Das Betriebssystem wurde aktualisiert.
  - Es wurden Konfigurationsänderungen vorgenommen.
  - Das Profil des Benutzers ist sehr groß. In diesem Fall ist auch die Profilladezeit hoch.
- Große Abweichung zwischen den Anmeldewerten des Benutzers (aktuelle und durchschnittliche Dauer) und der durchschnittlichen Dauer der Bereitstellungsgruppe.

Klicken Sie ggf. auf **Neu starten**, um den Anmeldeprozess des Benutzers zu beobachten und Probleme zu beheben, z. B. VM-Start oder Vermittlung.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Beheben von Anwendungsfehlern

Jul 08, 2016

Klicken Sie in der Ansicht Aktivitäts-Manager auf die Registerkarte Anwendungen. Sie können alle Anwendungen auf allen Maschinen anzeigen, auf die dieser Benutzer zugreifen kann, einschließlich der lokalen und der gehosteten Anwendungen für die derzeit verbundene Maschine und den aktuellen Status der einzelnen Maschine.
Hinweis: Wenn die Registerkarte Anwendungen abgeblendet ist, wenden Sie sich an einen Administrator, der die Berechtigung hat, die Registerkarte zu aktivieren.
Die Liste enthält nur die Anwendungen, die in der Sitzung gestartet wurden.

Für Serverbetriebssystemmaschinen und Desktopbetriebssystemmaschinen werden Anwendungen für jede getrennte Sitzung angezeigt. Wenn der Benutzer nicht verbunden ist, werden keine Anwendungen angezeigt.

| Aktion | Beschreibung |
|---|---|
| Beenden Sie die Anwendung, die nicht reagiert. | Wählen Sie die Anwendung aus, die nicht reagiert, und klicken Sie auf Anwendung beenden. Wenn die Anwendung beendet ist, fordern Sie den Benutzer auf, sie erneut zu starten. |
| Beenden Sie Prozesse, die nicht reagieren. | Wenn Sie die erforderlichen Berechtigungen haben, klicken Sie auf die Registerkarte Prozesse. Wählen Sie einen Prozess aus, der mit dieser Anwendung zusammenhängt oder der viele CPU-Ressourcen oder viel Speicher verbraucht, und klicken Sie auf Prozess beenden.<br>Wenn Sie nicht die erforderlichen Berechtigungen zum Beenden des Prozesses haben, schlägt das Beenden fehl. |
| Starten Sie die Maschine des Benutzers neu. | Nur Desktopbetriebssystemmaschinen: Klicken Sie für die ausgewählte Sitzung auf Neu starten. Sie können auch in der Ansicht Maschinendetails die Maschine mit den Energiesteuerelementen neu starten oder herunterfahren. Fordern Sie den Benutzer auf, sich neu anzumelden, sodass Sie die Anwendung überprüfen können.<br><br>Für Serverbetriebssystemmaschinen steht die Option "Neu starten" nicht zur Verfügung. Melden Sie stattdessen den Benutzer ab und fordern Sie ihn auf, sich neu anzumelden. |
| Setzen Sie die Maschine in den Wartungsmodus. | Wenn das Image einer Maschine gewartet werden muss, z. B. mit Patches oder anderen Updates, setzen Sie die Maschine in den Wartungsmodus und eskalieren Sie das Problem an den entsprechenden Administrator. Klicken Sie in der Ansicht Maschinendetails auf Details und aktivieren Sie die Option "Wartungsmodus". Eskalieren Sie an den entsprechenden Administrator. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Wiederherstellen von Desktopverbindungen

Jul 08, 2016

Überprüfen Sie von Director den Verbindungsstatus des Benutzers für die aktuelle Maschine in der Titelleiste des Benutzers.

Wenn die Desktopverbindung fehlgeschlagen ist, wird die Fehlerursache angezeigt, um Sie bei der Problembehandlung zu unterstützen.

| Aktion | Beschreibung |
| --- | --- |
| Stellen Sie sicher, dass die Maschine nicht im Wartungsmodus ist. | Achten Sie auf der Seite Benutzerdetails darauf, dass der Wartungsmodus deaktiviert ist. |
| Starten Sie die Maschine des Benutzers neu. | Wählen Sie die Maschine aus und klicken Sie auf Neu starten. Verwenden Sie diese Option, wenn die Maschine des Benutzers nicht mehr reagiert oder keine Verbindung herstellen kann, z. B. wenn die Maschine sehr viele CPU-Ressourcen verbraucht und dies die CPU unbrauchbar macht. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Wiederherstellen von Sitzungen

Jul 08, 2016

Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

Die Problembehandlung von Sitzungsfehlern machen Sie in der Ansicht Benutzerdetails im Bereich Sitzungsdetails. Sie können die Details der aktuellen Sitzung (durch die Sitzungs-ID gekennzeichnet) anzeigen.

| Aktion | Beschreibung |
|---|---|
| Beenden Sie Anwendungen und Prozesse, die nicht reagieren. | Klicken Sie auf die Registerkarte Anwendungen. Wählen Sie eine nicht reagierende Anwendung aus und klicken Sie auf Anwendung beenden. Sie können auch einen entsprechenden Prozess auswählen, der nicht reagiert, und auf Prozess beenden.<br>Beenden Sie auch Prozesse, die ungewöhnlich viel Speicher oder CPU-Ressourcen verbrauchen, da sie die CPU unbrauchbar machen können. |
| Trennen Sie die Windows-Sitzung. | Klicken Sie auf Sitzungssteuerung und wählen Sie dann Trennen. Diese Option steht nur für vermittelte Serverbetriebssystemmaschinen zur Verfügung. Für nicht vermittelte Sitzungen ist die Option deaktiviert. |
| Melden Sie den Benutzer von der Sitzung ab. | Klicken Sie auf Sitzungssteuerung und wählen Sie dann Abmelden. |

Zum Testen der Sitzung kann der Benutzer versuchen, sich neu anzumelden. Sie können den Benutzer auch spiegeln, um diese Sitzung genauer zu beobachten.

Hinweis: Wenn VDAs vor XenDesktop 7 auf Benutzergeräten ausgeführt werden, kann Director keine vollständigen Informationen über die Sitzung anzeigen. Stattdessen wird in einer Meldung angezeigt, dass die Informationen nicht verfügbar sind. Diese Meldungen werden möglicherweise auf der Seite Benutzerdetails und im Aktivitäts-Manager angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Ausführen von Systemberichten für HDX-Kanäle

Jul 08, 2016

Prüfen Sie in der Ansicht Benutzerdetails im Bereich HDX den Status der HDX-Kanäle auf der Maschine des Benutzers. Dieser Bereich ist nur verfügbar, wenn die Maschine des Benutzers mit HDX verbunden ist.
Wenn eine Meldung angibt, dass die Informationen zurzeit nicht verfügbar sind, warten Sie eine Minute, bis die Seite aktualisiert ist, oder klicken Sie auf die Schaltfläche Aktualisieren. Die Aktualisierung von HDX-Daten kann etwas länger dauern als bei anderen Daten.

Klicken Sie zur Anzeige weiterer Informationen auf das Fehler- oder Warnsymbol.

Tipp: Sie können Informationen über andere Kanäle in demselben Dialogfeld einblenden, indem Sie in der linken Ecke der Titelleiste auf den Pfeil nach links oder rechts klicken.
Systemberichte über die HDX-Kanäle werden hauptsächlich vom Citrix Support für die weitere Problembehandlung verwendet.

1. Klicken Sie im Bereich HDX auf Systembericht herunterladen.
2. Sie können die XML-Berichtdatei anzeigen oder speichern.
   - Klicken Sie zur Ansicht der XML-Datei auf Öffnen. Die XML-Datei wird in demselben Fenster wie die Anwendung Director angezeigt.
   - Klicken Sie zum Speichern der XML-Datei auf Speichern. Das Dialogfeld Speichern unter wird angezeigt, in dem Sie angeben, an welchem Speicherort auf der Director-Maschine die Datei heruntergeladen wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Zurücksetzen von Personal vDisk

Jul 08, 2016

Achtung: Beim Zurücksetzen der Disk werden die Einstellungen auf die werksseitigen Standardwerte zurückgesetzt und alle Daten, einschließlich der Anwendungen, werden gelöscht. Die Profildaten bleiben gespeichert, es sei denn, Sie haben den Personal vDisk-Standard geändert (d. h. das Umleiten der Profile vom Laufwerk C:) oder Sie verwenden keine Profillösung eines Drittanbieters.

Zum Zurücksetzen muss die Maschine mit Personal vDisk ausgeführt werden, der Benutzer muss aber nicht angemeldet sein.

Diese Option steht nur für Desktopbetriebssystemmaschinen zur Verfügung, sie ist für Serverbetriebssystemmaschinen deaktiviert.

1. Wählen Sie in der Ansicht Helpdesk die gewünschte Desktopbetriebssystemmaschine aus.
2. Klicken Sie in dieser Ansicht oder im Bereich Personalisierung der Ansicht Benutzerdetails auf Personal vDisk zurücksetzen.
3. Klicken Sie auf Zurücksetzen. Eine Warnmeldung gibt an, dass der Benutzer abgemeldet wird. Wenn der Benutzer abgemeldet ist (falls er angemeldet war), wird die Maschine neu gestartet.

Wenn das Zurücksetzen erfolgreich ist, wird im Feld Status im Bereich Personalisierung der Ansicht Benutzerdetails der Wert Wird ausgeführt angezeigt. Wenn das Zurücksetzen fehlgeschlagen ist, wird rechts neben Wird ausgeführt ein rotes X angezeigt. Wenn Sie auf dieses X zeigen, werden Informationen zu dem Fehler angezeigt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Zurücksetzen eines Benutzerprofils

Jul 08, 2016

Achtung: Wenn ein Profil zurückgesetzt wird, werden die Ordner und Dateien des Benutzers zwar gespeichert und in das neue Profil kopiert, aber die meisten Benutzerdaten werden gelöscht (z. B. wird die Registrierung zurückgesetzt und die Anwendungseinstellungen werden möglicherweise gelöscht).

1. Suchen Sie in Director den Benutzer, dessen Profil Sie zurücksetzen möchten, und wählen Sie seine Benutzersitzung aus.
2. Klicken Sie auf **Profil zurücksetzen**.
3. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
4. Fordern Sie den Benutzer auf, sich erneut anzumelden. Der Ordner und Dateien, die aus dem Profil des Benutzers gespeichert wurden, werden in das neue Profil kopiert.
   Wichtig: Wenn der Benutzer Profile auf mehreren Plattformen (z. B. Windows 8 und Windows 7) hat, fordern Sie den Benutzer auf, sich zuerst bei dem gleichen Desktop oder bei der gleichen App anzumelden, bei dem bzw. der dieser Benutzer Probleme hatte. Dies stellt sicher, dass das richtige Profil zurückgesetzt wird.
   Wenn das Profil ein Citrix Benutzerprofil ist, ist es zum Zeitpunkt der Benutzerdesktopanzeige bereits zurückgesetzt. Bei Microsoft-Roamingprofilen dauert die Ordnerwiederherstellung möglicherweise noch kurze Zeit an. Der Benutzer muss angemeldet bleiben, bis die Wiederherstellung abgeschlossen ist.

Hinweis: Bei den zuvor erläuterten Schritten wird davon ausgegangen, dass Sie XenDesktop (Desktop-VDA) verwenden. Wenn Sie XenApp (Server-VDA) verwenden, müssen Sie angemeldet sein, um das Profil zurückzusetzen. Der Benutzer muss sich dann abmelden und neu anmelden, um das Zurücksetzen des Profils abzuschließen.
Wenn das Profil nicht erfolgreich zurückgesetzt wird (z. B. der Benutzer kann sich nicht wieder anmelden oder einige der Dateien fehlen), müssen Sie das ursprüngliche Profil manuell wiederherstellen.
Die Ordner (und die Dateien) des Benutzerprofils werden gespeichert und in das neue Profil kopiert. Dabei gilt folgende Kopierreihenfolge:

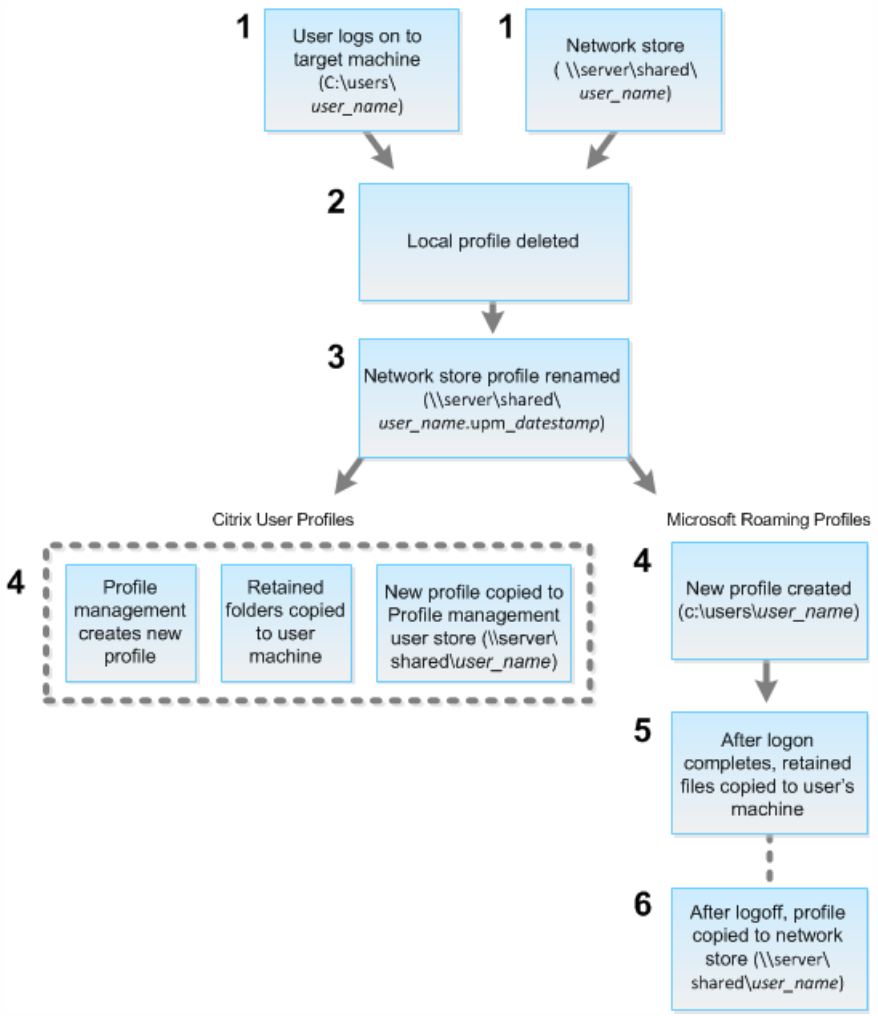
- Desktop
- Cookies
- Favoriten
- Dokumente
- Bilder
- Musik
- Videos

Hinweis: In Windows 8 und höheren Versionen werden Cookies beim Zurücksetzen des Profils nicht kopiert.

Alle Citrix Benutzerprofile oder Microsoft Roamingprofile können zurückgesetzt werden. Wenn der Benutzer sich abmeldet und Sie den Befehl zum Zurücksetzen wählen (entweder in Director oder mit dem PowerShell SDK), identifiziert Director zunächst das verwendete Benutzerprofil und gibt dann den entsprechenden Befehl zum Zurücksetzen. Director erhält die Informationen über die Profilverwaltung, einschließlich Informationen zur Profilgröße, zum Typ und den Anmeldezeiten.

In diesem Diagramm wird die Verarbeitung dargestellt, die bei der nächsten Benutzeranmeldung ausgeführt wird.


© 1999-2017 Citrix Systems, Inc. All rights reserved.




1. Der Befehl zum Zurücksetzen von Director gibt den Profiltyp an. Der Profilverwaltungsdienst versucht dann, ein Profil dieses Typs zurückzusetzen und sucht die entsprechende Netzwerkfreigabe (Benutzerspeicher). Wenn der Benutzer von der Profilverwaltung verarbeitet wird, aber einen Roamingprofilbefehl erhält, wird er abgelehnt (oder umgekehrt).
2. Wenn ein lokales Profil vorhanden ist, wird es gelöscht.
3. Das Netzwerkprofil wird umbenannt.
4. Die nächste Aktion hängt davon ab, ob es sich bei dem Profil, das zurückgesetzt wird, um ein Citrix Benutzerprofil oder ein Microsoft Roamingprofil handelt.
   - Für Citrix Benutzerprofile wird das neue Profil mit den Importregeln der Profilverwaltung erstellt, die Ordner werden in das Netzwerkprofil zurückkopiert und der Benutzer kann die Anmeldung wie gewohnt fortsetzen. Wenn ein Roamingprofil für das Zurücksetzen verwendet wird, bleiben alle Registrierungseinstellungen im Roamingprofil im zurückgesetzten Profil gespeichert.
     Hinweis: Sie können in der Profilverwaltung konfigurieren, dass das Roamingprofil ggf. von einem Vorlagenprofil überschrieben wird.
   - Für Microsoft Roamingprofile wird ein neues Profil von Windows erstellt, und die Ordner werden bei Anmeldung des Benutzers auf das Benutzergerät zurückkopiert. Bei der nächsten Benutzerabmeldung wird das neue Profil in den Netzwerkspeicher kopiert.

1. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
2. Löschen Sie das lokale Profil, falls vorhanden.
3. Suchen Sie den archivierten Ordner auf der Netzwerkfreigabe, bei dem das Datum und die Uhrzeit dem Ordnernamen


© 1999-2017 Citrix Systems, Inc. All rights reserved.

angehängt wurden, also den Ordner mit der Erweiterung .upm_Datumsstempel.

4. Löschen Sie den aktuellen Profilnamen, d. h. die Datei ohne die Erweiterung upm_Datumsstempel.
5. Benennen Sie den archivierten Ordner in den ursprünglichen Profilnamen um (entfernen Sie den Datumsstempel). Sie haben das Profil auf den ursprünglichen Zustand zurückgesetzt.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# SDKs und APIs

Aug 17, 2016

Das aktuelle Release enthält mehrere SDKs und APIs.

**SDK für XenApp und XenDesktop:** Dieses basiert auf zahlreichen Microsoft Windows PowerShell 3.0-Snap-Ins, mit dem Sie die gleichen Tasks wie mit der Citrix Studio-Konsole und andere Tasks ausführen können, die in Studio allein nicht möglich sind.

Weitere Informationen finden Sie unter Citrix Developer.

**Citrix Group Policy SDK:** Mit diesem SDK können Sie Einstellungen und Filter für Gruppenrichtlinien anzeigen und konfigurieren. Es verwendet einen PowerShell-Anbieter, um einen virtuellen Datenträger zu erstellen, der mit den Maschinen- und Benutzereinstellungen und -filtern übereinstimmt. Der Anbieter wird als Erweiterung zu New-PSDrive angezeigt. Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein. Weitere Informationen finden Sie Abschnitt Group Policy SDK weiter unten.

**Überwachungsdienst-OData-API:** Diese API können Sie für Folgendes verwenden:

- Analysieren historischer Trends für die Planung
- Durchführen einer eingehenden Problembehandlung bei Verbindungs- und Maschinenfehlern
- Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse, z. B. wenn PowerPivot-Tabellen in Microsoft Excel für die Anzeige von Daten auf verschiedene Weise verwendet werden
- Erstellen einer benutzerdefinierten Benutzeroberfläche auf der Basis der von der API bereitgestellten Daten

Weitere Informationen finden Sie in den Artikeln zur Überwachungsdienst-OData-API.

# XenApp- und XenDesktop-SDK

Ab Version 7.x bieten XenApp und XenDesktop mit FlexCast Management Architecture eine einheitliche Architektur und Verwaltung. Daher stehen nun in XenApp viele Features bereit, die es zuvor nur in XenDesktop gab. Elemente des SDKs für gemeinsame Features gelten also nun sowohl für XenApp als auch für XenDesktop, selbst wenn die Befehle sich nur auf XenDesktop beziehen.

In der folgenden Liste werden die Unterschiede zwischen Version 5 und 7.x des SDKs für XenApp und XenDesktop aufgeführt.

- **Neues High-Level-SDK**: XenDesktop 7 umfasst ein neues High-Level-SDK, mit dem Sie schnell und mühelos ein Skript erstellen und die Siteerstellung und -wartung automatisieren. Das High-Level-SDK isoliert Sie von der Komplexität der Low-Level-SDKs, sodass Sie für das Erstellen einer neuen Site nur zwei Cmdlets ausführen müssen.
- **Neue Low-Level-SDKs**: Einzelne Low-Level-SDKs werden für die neuen XenDesktop 7-Dienste bereitgestellt, u. a. ein dediziertes und verbessertes SDK für den Dienst für die delegierte Administration (DAS), das vorher Teil des Broker-SDKs in XenDesktop 5 war. Es gibt auch SDKs für neue Features, u. a. Überwachungsdienst, Umgebungstest und Konfigurationsprotokollierung.
- **Kataloge und Bereitstellungsgruppen für Windows-Serverbetriebssystemmaschine**: Mit dem XenDesktop 7-SDK stellen Sie kostengünstig Anwendungen und Desktops bereit, die auf Serverbetriebssystemen gehostet werden.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Anwendungen für Desktopbetriebssystemmaschinen**: Anwendungen für Desktopbetriebssystemmaschinen haben sich auf SDK-Ebene wesentlich geändert. Wenn Sie vorhandene Skripts für die Ausführung von Anwendungen auf Desktopbetriebssystemen haben, müssen Sie diese Skripts für XenDesktop 7 aktualisieren, da es fast keine Rückwärtskompatibilität gibt.
- **Anwenden von Einstellungen auf Maschinen in Bereitstellungsgruppen**: In XenDesktop 7 können Sie mit Konfigurationsslots Einstellungen auf Maschinen in einer bestimmten Bereitstellungsgruppe statt auf alle Maschinen in einer Site anwenden. So können Sie für eine bestimmte Bereitstellungsgruppe konfigurieren, welche Einstellungen für diese Gruppe gelten. Zahlreiche vordefinierte Konfigurationsslots werden bereitgestellt, die unterschiedliche Typen von Einstellungen enthalten, u. a. Einstellungen für StoreFront-Adressen, die mit Speicherorten von Receiver- oder App-V-Veröffentlichungserver verwendet werden. Eine Sammlung von Einstellungen kann sich nur auf eine bestimmte Bereitstellungsgruppe auswirken, und eine andere Sammlung von Einstellungen von dem gleichen Slot wirkt sich auf eine andere Bereitstellungsgruppe aus. Sie können Namen verwenden, die für Ihre Bereitstellung geeignet sind, z. B. "Vertriebsabteilungsrichtlinie".
- **Ersetzte Katalogtypen**: In XenDesktop 7 wurden Katalogtypen durch Kataloge mit individuellen Eigenschaften ersetzt. Für die Rückwärtskompatibilität können Sie weiterhin vorhandene Skripts nutzen, die Katalogtypen verwenden, z. B. ein Image (gepoolt) und Thin Clone (dediziert) usw., intern werden diese jedoch in Gruppen von Eigenschaften konvertiert.
  **Achtung:** Die Rückwärtskompatibilität mit XenDesktop 5-Katalogtypen wurde beibehalten, wenn es praktikabel war. Verwenden Sie beim Schreiben neuer Skripts jedoch keine Katalogtypen sondern geben Sie Kataloge mit individuellen Eigenschaften an.

- **Ersetztes Desktopobjekte**: In XenDesktop 5 ist das Desktopobjekt einer der Haupttypen des SDK-Objekts, das in Broker-SDK-Skripts verwendet wird. Das Desktopobjekt beschreibt sowohl die Maschine als auch die Sitzung auf der Maschine. In XenDesktop 7 wird dieses Objekt durch das Sitzungsobjekt und das Maschinenobjekt ersetzt, die beide erweitert wurden und jetzt die Funktion des Desktopobjekts übernehmen. Für die Rückwärtskompatibilität können Sie jedoch weiterhin vorhandene Skripts verwenden, die das Desktopobjekt nutzen.
  **Achtung:** Die Rückwärtskompatibilität mit XenDesktop 5 wurde beibehalten, wenn es praktikabel war. Verwenden Sie beim Schreiben neuer Skripts jedoch nicht das Desktopobjekt, sondern geben Sie Sitzungs- und Maschinenobjekte an.

Die Richtlinienregeln im SDK und der Studio-Konsole sind nicht identisch. Anspruchs- und Zuordnungsrichtlinienregeln sind unabhängige Entitäten im SDK, und in der Konsole. Diese Entitäten sind nicht sichtbar, da sie nahtlos mit der Bereitstellungsgruppe zusammengeführt werden. Weiterhin sind Richtlinienregeln im SDK weniger restriktiv.

Das SDK enthält mehrere PowerShell-Snap-Ins, die automatisch vom Installationsassistenten installiert werden, wenn Sie den Delivery Controller oder Studio installieren.

Berechtigungen: Sie müssen die Shell oder das Skript mit einer ID ausführen, die über Citrix Administratorrechte verfügt. Obwohl die Mitglieder der lokalen Administratorgruppe auf dem Controller automatisch über Volladministratorprivilegien verfügen, um XenApp bzw. XenDesktop zu installieren, empfiehlt Citrix, dass Sie für den normalen Betrieb Citrix Administratoren mit den entsprechenden Rechten erstellen und nicht das lokale Administratorkonto verwenden. Wenn Sie Windows Server 2008 R2 ausführen, müssen Sie die Shell oder das Skript als Citrix Administrator und nicht als Mitglied der lokalen Administratorgruppe ausführen.

Zugreifen auf die Cmdlets:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Starten einer Shell in PowerShell 3.0: Öffnen Sie Studio, wählen Sie die Registerkarte **PowerShell** und klicken Sie auf **PowerShell starten**.
2. Legen Sie die Ausführungsrichtlinie in PowerShell fest, um SDK-Cmdlets in Skripts zu verwenden. Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Dokumentation von Microsoft.
3. Fügen Sie mit dem Cmdlet **Add -PSSnapin** in der Windows PowerShell-Konsole die Snap-Ins hinzu, die Sie in der PowerShell-Umgebung benötigen.

   V1 und V2 beziehen sich auf die Version des Snap-Ins. (XenDesktop 5-Snap-Ins sind Version 1; XenDesktop 7-Snap-Ins sind Version 2. Zum Installieren von XenDesktop 7-Snap-Ins geben Sie beispielsweise "Add-PSSnapin Citrix.ADIdentity.Admin.V2" ein.) Geben Sie zum Importieren aller Cmdlets "Add-PSSnapin Citrix.*.Admin.V*" ein.

Nach dem Hinzufügen der Snap-Ins, können Sie auf die Cmdlets und die zugehörige Hilfe zugreifen.

**Hinweis:** Auf folgende Weise zeigen Sie die aktuelle XenApp- und XenDesktop-Hilfe zu PowerShell-Cmdlets an:

1. Fügen Sie mit der PowerShell-Konsole folgende Citrix Snap-Ins hinzu: Add –PSSnapin Citrix.*.Admin.V*.
2. Folgen Sie den Anweisungen in PowerShell Integrated Scripting Environment (ISE).

# Group Policy SDKs

Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein.

Zum Hinzufügen des Group Policy SDKs geben Sie **Add-PSSnapin citrix.common.grouppolicy** ein. (Zum Aufrufen der Hilfe geben Sie **help New-PSDrive -path localgpo:/** ein.)

Zum Erstellen einer virtuellen Festplatte und Laden dieser Festplatte mit Einstellungen geben Sie Folgendes ein: **New-PSDrive** <*Standardparameter*> **[-PSProvider] CitrixGroupPolicy -Controller** <*Zeichenfolge*> , wobei die Controller-Zeichenfolge der vollqualifizierte Domänenname eines Controllers in der Site ist, aus der die Einstellungen geladen werden sollen.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Überwachungsdienst-OData-API

Jul 08, 2016

Zusätzlich zur Anzeige von historischen Daten in der Citrix Director-Konsole können Sie Daten mit der Überwachungsdienst-OData-API abfragen. Sie können die API für Folgendes verwenden:

- Analysieren historischer Trends für die Planung
- Durchführen einer eingehenden Problembehandlung bei Verbindungs- und Maschinenfehlern
- Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse, z. B. wenn PowerPivot-Tabellen in Microsoft Excel für die Anzeige von Daten auf verschiedene Weise verwendet werden
- Erstellen einer benutzerdefinierten Benutzeroberfläche auf der Basis der von der API bereitgestellten Daten

Die Überwachungsdienst-OData-API verwendet das Open Data-Protokoll (OData), ein Webprotokoll für die Abfrage und Aktualisierung von Daten, das auf Webtechnologien wie HTTP aufbaut. Weitere Informationen über das OData-Protokoll finden Sie unter http://www.odata.org.

Die Überwachungsdienst-API setzt mit den Windows Communication Foundation (WCF) Data Services auf SQL Server-Datenbanken auf, die während der Verarbeitung und Konsolidierung aufgefüllt werden. Bei Verwendung von WCF mit wsHttpBinding werden zwei Endpunkte verfügbar gemacht. Die Basisadresse ist http:// {dc-host}/Citrix/Monitor/OData/v2. Sie können Endpunkte auch mit TLS schützen (weitere Informationen finden Sie unter Schützen von Endpunkten mit TLS).

1. Der Endpunkt "Data" gestattet direkten Lesezugriff auf die Datenbankentitäten, Zugriff ist mit der Abfragesprache OData möglich. Dieser Endpunkt gestattet einen sehr flexiblen Zugriff im Hinblick auf Filter- und Spaltenauswahl. Die URI der Data-API ist: http://{dc-host}/Citrix/Monitor/OData/v2/Data. Weitere Informationen über den Zugriff auf Monitor Service-Daten finden Sie unter Zugriff auf Daten mit der API.
2. Der Endpunkt "Methods" macht Dienstvorgänge verfügbar, die von Citrix Director für das Abrufen von Daten verwendet werden, die eine komplexe Gruppierung und hohe Leistungsstandards erfordern (z. B. Abfragen für das Dashboard und Trend-Seiten). Die URI der Methods-API ist: http://{dc-host}/Citrix/Monitor/OData/v2/Methods. Methoden werden nur in Director selbst verwendet, d. h. nicht von der Mehrheit der Citrix Kunden. Sie werden daher hier nicht dokumentiert.

Die in XenApp und XenDesktop 7.6 enthaltene API-Version bietet die folgenden neuen Features:

- **Hotfix-Bestand** In der Ansicht "Benutzerdetails" oder „Maschine“ in Director können Sie eine Liste aller Citrix Hotfixes anzeigen, die auf einer Maschine installiert wurden. Sie können mit der API diese Daten extrahieren und benutzerdefinierte Berichte erstellen (z. B. Status der installierten Hotfixes über eine ganze Site) oder sie in eine Analyticsengine ziehen. Neue Klassen wurden eingeführt und die Maschinenklasse unterstützt nun die Nachverfolgung von auf dem Controller und VDAs installierten Citrix Hotfixes.
- **Anonyme Sitzungsproblembehandlung.** Sitzungen können in Form gepoolter lokaler Benutzerkonten ausgeführt werden. Die API hat eine neue IsAnonymous-Eigenschaft für die Sitzungsklasse (Standardwert = FALSE).
- **Bericht über die Verwendung gehosteter Anwendungen.** Director bietet neue Kapazitätsberichte zur Verwendung gehosteter Anwendungen über bestimmte Zeiträume. Mit der API können Sie Berichte zu den Details jeder in einer Benutzersitzung ausgeführten Anwendungsinstanz erstellen.

Alle die Daten betreffenden Updates sind in der API-Referenz unter http://support.citrix.com/help/monitorserviceapi/7.6/ vollständig dokumentiert.

Die Methode "GetSessionSummary" ist seit diesem Release veraltet.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Zugriff auf Daten mit der API

Jun 16, 2016

Die folgenden Datentypen sind über die Überwachungsdienst-API verfügbar:

- Daten zu Verbindungsfehlern
- Maschinen in fehlerhaftem Zustand
- Sitzungsnutzung
- Anmeldedauer
- Daten zum Lastausgleich
- Auf eine Maschine angewendete Hotfixes
- Verwendung gehostete Anwendung

Eine komplette Beschreibung der Datenobjekte finden Sie unter http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/.

Zur Verwendung der Überwachungsdienst-OData-API müssen Sie XenApp- bzw. XenDesktop-Administrator sein. Zum Aufrufen der API ist Lesezugriff erforderlich. Welche Daten zurückgegeben werden, hängt von den Rollen und Berechtigungen des XenApp- bzw. XenDesktop-Administrators ab. Administratoren von Bereitstellungsgruppen können beispielsweise die Überwachungsdienst-API aufrufen, aber die zurückgegebenen Daten hängen von dem mit Citrix Studio eingerichteten Bereitstellungsgruppenzugriff ab. Weitere Informationen über XenApp-/XenDesktop-Administratorrollen und -berechtigungen finden Sie unter Delegierte Administration.

### Abfragen der Daten

Die Überwachungsdienst-API ist eine REST-basierte API, auf die mit einem OData-Consumer zugegriffen werden kann. OData-Consumer sind Anwendungen, die mit dem OData-Protokoll verfügbar gemachte Daten nutzen. OData-Consumer reichen vom einfachen Webbrowser bis zur benutzerdefinierten Anwendung, die sämtliche Features des OData-Protokolls nutzt. Weitere Informationen über OData-Consumer finden Sie unter http://www.odata.org/ecosystem#consumers.

Jeder Teil des Überwachungsdienst-Datenmodells ist zugänglich und kann über die URL gefiltert werden. OData bietet eine Abfragesprache im URL-Format zum Abrufen von Einträgen aus einem Dienst. Weitere Informationen finden Sie unter http://msdn.microsoft.com/en-us/library/ff478141.aspx.

Die Abfrage wird serverseitig verarbeitet und kann clientseitig mit dem OData-Protokoll weiter gefiltert werden.

Die modellierten Daten fallen in drei Hauptkategorien: Aggregierte Daten (die Zusammenfassungstabellen), aktueller Zustand von Objekten (Maschinen, Sitzungen usw.) und Protokolldaten, wobei es sich um historische Ereignisse handelt (z. B. Verbindungen).

Hinweis: Enumerationen werden vom OData-Protokoll nicht unterstützt, stattdessen werden ganze Zahlen verwendet. Weitere Informationen zum Bestimmen der von der Überwachungsdienst-OData-API zurückgegebenen Werte finden Sie unter http://support.citrix.com/help/monitorserviceapi/7.6/.

### Aggregation der Datenwerte

Der Überwachungsdienst erfasst diverse Daten über Benutzersitzungsnutzung, Benutzeranmeldeleistung, Sitzungslastausgleich und zu Fehlern bei Verbindungen und Maschinen. Die Daten werden je nach Kategorie unterschiedlich aggregiert. Zum Interpretieren der Daten sind Kenntnisse über die Aggregation der mit den OData-Methoden-APIs abgerufenen Datenwerte unverzichtbar. Beispiel:


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Fehler bei verbundenen Sitzungen und Maschinen treten in einem bestimmten Zeitraum auf und werden daher als Höchstwerte in einem Zeitraum verfügbar gemacht.
- Die Anmeldedauer ist ein Zeitlängenwert und wird daher als Durchschnitt in einem Zeitraum verfügbar gemacht.
- Die Anzahl der Anmeldungen und Verbindungsfehler repräsentieren eine Anzahl von Vorkommen in einem bestimmten Zeitraum und werden als Summen in einem Zeitraum gemacht.

### Auswertung gleichzeitiger Daten

Sitzungen müssen sich überschneiden, um als gleichzeitig angesehen zu werden. Bei einem Zeitintervall von 1 Minute werden jedoch alle Sitzungen in dieser Minute (mit oder ohne Überschneidung) als gleichzeitig angesehen, d. h. das Intervall ist so klein, dass sich der Mehraufwand für die Berechnung der Genauigkeit nicht lohnt. Finden die Sitzungen in der gleichen Stunde, aber nicht in der gleichen Minute statt, werden sie als einander nicht überschneidend angesehen.

### Korrelation der Zusammenfassungstabellen mit Rohdaten

Das Datenmodell stellt Metriken auf zwei verschiedene Arten dar:

- Die Zusammenfassungstabellen zeigen aggregierte Ansichten der Metriken in Granularitäten pro Minute, Stunde und Tag an.
- Die Rohdaten stehen für einzelne Ereignisse oder den aktuellen Zustand, der bzw. die für eine Sitzung, Verbindung, Anwendung und andere Objekte protokolliert werden.

Wenn Sie versuchen, Daten über API-Aufrufe hinweg oder innerhalb des Datenmodells selbst zu korrelieren, sollten Sie die folgenden Konzepte und Einschränkungen kennen:

- **Keine Zusammenfassungsdaten für Teilintervalle:** Die Zusammenfassungen von Metriken erfüllen die Anforderungen von historischen Trends über lange Zeiträume hinweg. Diese Metriken werden für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Für Teilintervalle am Anfang (die ältesten verfügbaren Daten) und am Ende der Datensammlung gibt es keine Zusammenfassungsdaten. Beim Anzeigen der Aggregation eines Tages (Intervall=1440) bedeutet dies, dass der erste Tag und der aktuelle unvollständige Tag keine Daten aufweisen. Obwohl für diese Teilintervalle u. U. Rohdaten vorhanden sind, werden sie nie zusammengefasst. Sie können das früheste und letzte Aggregationsintervall für eine bestimmte Datengranularität festlegen, indem Sie die Mindest- und Höchstwerte für "SummaryDate" aus einer bestimmten Zusammenfassungstabelle nehmen. Die Spalte "SummaryDate" stellt den Start des Intervalls dar. Die Spalte "Granularity" steht für die Länge des Intervalls der aggregierten Daten.
- **Korrelation nach Zeit:** Metriken werden, wie oben beschrieben, für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Sie können für historische Trends verwendet werden, aber rohe Ereignisdaten stellen möglicherweise einen aktuelleren Zustand dar als die Zusammenfassung für die Trendanalyse. Bei zeitbasierten Vergleichen zwischen der Zusammenfassung und den Rohdaten muss beachtet werden, dass es keine Zusammenfassungsdaten für Teilintervalle gibt, die am Anfang und Ende des Zeitraums auftreten.
- **Verpasste und latente Ereignisse:** Wenn Ereignisse verpasst werden oder während des Aggregationszeitraums latent sind, sind die für die Zusammenfassungstabelle aggregierten Metriken möglicherweise ungenau. Obwohl der Überwachungsdienst versucht, einen genauen aktuellen Zustand zu erhalten, wird die Aggregation für verpasste oder latente Ereignisse nicht im Nachhinein neu für die Zusammenfassungstabellen berechnet.
- **Hochverfügbare Verbindungen:** Bei hoher Verfügbarkeit von Verbindungen entstehen in den Zusammenfassungsdaten für aktuelle Verbindungen Lücken, aber die Sitzungsinstanzen werden dennoch in den Rohdaten ausgeführt.
- **Beibehaltungszeitraum für Daten:** Daten werden in den Zusammenfassungstabellen basierend auf einem anderen Bereinigungszeitplan beibehalten als Rohdaten von Ereignissen. Daten fehlen möglicherweise, weil die Zusammenfassungstabellen oder die unformatierten Tabellen bereinigt wurde. Beibehaltungszeiträume können


© 1999-2017 Citrix Systems, Inc. All rights reserved.

unterschiedliche Granularitäten für Zusammenfassungsdaten aufweisen. Daten basierend auf niedrigerer Granularität (Minuten) werden schneller bereinigt als Daten, die auf höherer Granularität (Tage) basieren. Wenn Daten bereinigt wurden und in einer Granularitätskategorie fehlen, sind sie möglicherweise in einer höheren Granularitätskategorie. API-Aufrufe geben nur Daten für die angeforderte Granularität zurück. Wenn für eine Granularität keine Daten zurückgegeben werden, sind möglicherweise für den gleichen Zeitraum Daten für eine höhere Granularität vorhanden.

- **Zeitzonen:** Metriken werden mit UTC-Zeitstempeln gespeichert. Zusammenfassungstabellen werden basierend auf stündlichen Zeitzonengrenzen aggregiert. Bei Zeitzonen, die nicht in diese stündlichen Grenzen fallen, gibt es möglicherweise Unstimmigkeiten beim Ort der Datenaggregation.

### Datengranularität und -beibehaltung

Die Granularität der aggregierten Daten, die von Director abgerufen werden, ist eine Funktion des angeforderten Zeitraums (T). Folgende Regeln gelten:

- 0 < T <= 1 Stunde: minutengenaue Granularität wird verwendet
- 0 <=30 Tage: stundengenaue Granularität wird verwendet
- T > 31 Tage: tagesgenaue Granularität wird verwendet

Angeforderte Daten, die nicht von aggregierten Daten stammen, stammen von den rohen Sitzungs- und Verbindungsinformationen. Diese Menge dieser Daten nimmt schnell zu, daher haben sie eine eigene Bereinigungseinstellung. Bereinigung gewährleistet, dass nur relevante Daten langfristig gespeichert werden. Damit wird eine bessere Leistung sichergestellt, während die für die Berichterstellung erforderliche Granularität beibehalten werden kann. Bei Kunden, die keine Lizenz für die Platinum Edition haben, beginnt die Bereinigung am 8. Tag, unabhängig vom Standardbereinigungszeitraum. Platinum-Kunden können den Beibehaltungszeitraum auf die gewünschte Anzahl an Tagen einstellen, sonst wird der Standardwert verwendet.

Mit den folgenden Einstellungen wird die Bereinigung gesteuert:

| Einstellungsname | Betroffene Bereinigung | Standardwert (Tage) | Zugriff mit |
|---|---|---|---|
| GroomSessionsRetentionDays | Sitzungs- und Sitzungsdetaileinträge | 7 für Nicht-Platinum-Benutzer, 90 für Platinum | Cmdlet (set/get-monitorconfiguration) |
| GroomSummariesRetentionDays | Einträge für DesktopGroupSummary, FailureLogSummary und LoadIndexSummary. Aggregierte Daten, tägliche Granularität | 7 für Nicht-Platinum-Benutzer, 90 für Platinum | Cmdlet (set/get-monitorconfiguration) |
| GroomHourlyRetentionDays | Aggregierte Daten - stundengenaue Granularität | 32 Tage | Monitor.Configuration Database Table. Siehe Hinweis unten. |
| GroomMinuteRetentionDays | Aggregierte Daten - minutengenaue Granularität | 3 Tage | Monitor.Configuration Database Table. Siehe Hinweis unten. |


© 1999-2017 Citrix Systems, Inc. All rights reserved.

| Einstellungsname | Betroffene Bereinigung | Standardwert (Tage) | Zugriff mit |
|---|---|---|---|
| GroomFailuresRetentionDays | Einträge für MachineFailureLog und ConnectionFailureLog | 7 für Nicht-Platinum-Benutzer, 90 für Platinum | Cmdlet (set/get-monitorconfiguration) |
| GroomLoadIndexesRetentionDays | Einträge für LoadIndex | 7 für Nicht-Platinum-Benutzer, 90 für Platinum | Cmdlet (set/get-monitorconfiguration) |
| GroomDeletedRetentionDays | Maschinen-, Katalog-, Desktopgruppen- und Hypervisorentitäten, die einen LifecycleState von "Deleted" haben. Dadurch werden auch zugehörige Einträge für Sitzung, Sitzungsdetail, Zusammenfassung, Fehler oder LoadIndex gelöscht. | 7 für Nicht-Platinum-Benutzer, 90 für Platinum | Cmdlet (set/get-monitorconfiguration) |
| GroomMachineHotfixHistoryRetentionDays | Auf VDA und Controllermaschinen angewendete Hotfixes | 90 für Nicht-Platinum- und Platinum-Benutzer | Cmdlet (set/get-monitorconfiguration) |

Achtung: Nach dem Ändern von Werten auf der Überwachungsdienstdatenbank ist ein Neustart des Diensts erforderlich, damit die neuen Werte wirksam werden. Führen Sie Änderungen an der Überwachungsdienstdatenbank nur mit Anleitung vom Citrix Support durch.

Das Beibehalten von Daten über lange Zeiträume hinweg hat die folgenden Auswirkungen auf die Größe von Tabellen:

- **Stundengenaue Daten:** Wenn Sie stundengenaue Daten bis zu zwei Jahre lang in der Datenbank speichern, wächst die Datenbank einer Site mit 1000 Bereitstellungsgruppen ungefähr wie folgt an:
  1000 Bereitstellungsgruppen x 24 Stunden/Tag x 365 Tage/Jahr x 2 Jahre = 17.520.000 Datenreihen. Diese große Datenmenge in den Aggregationstabellen hat beträchtliche Auswirkungen auf die Leistung. Wenn man bedenkt, dass die Dashboarddaten aus dieser Tabelle gezogen werden, sind die Anforderungen an den Datenbankserver möglicherweise riesig. Übermäßig viele Daten können dramatische Auswirkungen auf die Leistung haben.

- **Sitzungs- und Ereignisdaten:** Diese Daten werden jedes Mal gesammelt, wenn eine Sitzung gestartet und eine Verbindung/Wiederverbindung hergestellt wird. Bei einer großen Site (100.000 Benutzer) nimmt die Menge dieser Daten sehr schnell zu. Beispielsweise entsprechen die über zwei Jahre gespeicherten Tabellen mehr als 1 TB Daten und erfordern eine High-End-Unternehmensdatenbank.


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Schützen von Endpunkten mit TLS

Jun 16, 2016

In diesem Dokument wird erläutert, wie Sie die Endpunkte der Überwachungsdienst-OData-API mit TLS schützen. Wenn Sie TLS verwenden, müssen Sie TLS auf allen Delivery Controllern in der Site konfigurieren. Sie können keine Mischung aus Controllern mit und ohne TLS verwenden.

Zum Schützen der Endpunkte des Überwachungsdiensts mit TLS müssen Sie die folgende Konfiguration vornehmen. Einige Schritte müssen nur einmal pro Site vorgenommen werden, andere hingegen auf jeder Maschine, auf der der Überwachungsdienst gehostet wird. Die Schritte werden nachfolgend beschrieben.

**Teil 1: Zertifikatregistrierung im System**

1. Erstellen Sie mit einem vertrauenswürdigen Zertifikat-Manager ein Zertifikat. Das Zertifikat muss dem Port auf der Maschine zugeordnet werden, den Sie für OData TLS verwenden möchten.
2. Konfigurieren Sie den Überwachungsdienst zur Verwendung dieses Ports für TLS-Kommunikation. Die Schritte hängen von der jeweiligen Umgebung ab und davon, wie diese mit Zertifikaten funktioniert. Das folgende Beispiel zeigt das Konfigurieren von Port 449:

- Ordnen Sie das Zertifikat einem Port zu:
  netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9  appid='{00000000-0000-0000-0000-000000000000}'
  Tipp: Stellen Sie in einem PowerShell-Befehlsfenster sicher, dass Sie die GUID in der Anwendungs-ID mit einfachen Anführungszeichen wie oben dargestellt einschließen, da der Befehl sonst nicht funktioniert. Beachten Sie, dass diesem Beispiel eine Zeile für bessere Lesbarkeit hinzugefügt wurde.

**Teil 2: Ändern der Konfigurationseinstellungen des Überwachungsdiensts**

1. Führen Sie auf jedem Delivery Controller in der Site folgende PowerShell-Befehle einmal aus. Damit wird die Registrierung des Überwachungsdiensts beim Konfigurationsdienst aufgehoben.
   asnp citrix.*  $serviceGroup = get-configregisteredserviceinstance -servicetype Monitor | Select -First 1 ServiceGroupUid  remove-configserviceGroup -ServiceGroupUid $serviceGroup.ServiceGroupU
2. Führen Sie den folgenden Schritt auf allen Controllern in der Site aus:
   - Verwenden Sie eine Eingabeaufforderung zum Suchen des Verzeichnisses des installierten Citrix Überwachungsdiensts (in der Regel C:\Programme\Citrix\Monitor\Service). Führen Sie in diesem Verzeichnis Folgendes aus:
     Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl
   - Führen Sie die folgenden PowerShell-Befehle aus:
   asnp citrix.*  (if not already run within this window)  get-MonitorServiceInstance | register-ConfigServiceInstance  Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGro


© 1999-2017 Citrix Systems, Inc. All rights reserved.

# Beispiele

Jun 16, 2016

Die folgenden Beispiele zeigen, wie Daten mit der Überwachungsdienst-OData-API exportiert werden.

### Beispiel 1 – unformatiertes XML

1. Geben Sie die URL für jede Datengruppe in einen Webbrowser ein, der mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten ausgeführt wird. Citrix empfiehlt die Verwendung des Chrome-Browsers mit dem Add-In Advanced Rest Client.
2. Zeigen Sie die Quelle an.

### Beispiel 2 - PowerPivot für Excel

Bei diesen Anweisungen wird davon ausgegangen, dass Sie Microsoft Excel und PowerPivot bereits installiert haben.

Öffnen Sie Excel mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten.

Bei Verwendung von Excel 2010:

1. Klicken Sie auf der Registerkarte "PowerPivot".
2. Klicken Sie auf "PowerPivot-Fenster".
3. Klicken Sie im Menüband auf **Aus Datenfeeds**.
4. Wählen Sie einen Anzeigenamen für die Verbindung aus (z. B. XenDesktop-Überwachungsdaten) und geben Sie die Datenfeed-URL ein: http://{dc-host}/Citrix/Monitor/OData/v1/Data (oder "https:", falls Sie TLS verwenden).
5. Klicken Sie auf **Next**.
6. Wählen Sie die Tabellen aus, die Sie in Excel importieren möchten, und klicken Sie auf **Fertig stellen**. Die Daten werden abgerufen.
7. Sie können die Daten jetzt über PowerPivot mit PivotTables und PivotCharts anzeigen und analysieren. Weitere Informationen finden Sie im Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx.

Bei Verwendung von Excel 2013:

1. Klicken Sie auf die Registerkarte "Daten".
2. Wählen Sie "Aus anderen Quellen > Aus OData-Datenfeed".
3. Geben Sie die URL des Datenfeeds ein: http://{dc-host}/Citrix/Monitor/OData/v1/Data (oder "https:", wenn Sie TLS verwenden) und klicken Sie auf **Weiter**.
4. Wählen Sie die Tabellen aus, die Sie in Excel importieren möchten, und klicken Sie auf **Weiter**.
5. Akzeptieren Sie die Standardnamen oder passen Sie Namen an und klicken Sie auf **Fertig stellen**.
6. Wählen Sie **Nur Verbindung** oder **Pivot Report**. Die Daten werden abgerufen.
7. Sie können die Daten jetzt über PowerPivot mit PivotTables und PivotCharts anzeigen und analysieren. Weitere Informationen finden Sie im Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx.

### Beispiel 3 – LINQPad

Bei diesen Anweisungen wird davon ausgegangen, dass Sie LINQPad bereits installiert haben.

1. Führen Sie LinqPad mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten aus.
   Tipp: Die einfachste Methode ist Download, Installation und Ausführung auf dem Delivery Controller.
2. Klicken Sie auf den Link "Add connection".


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie "WCF Data Services 5.1 (OData 3)" und klicken Sie auf **Weiter**.
4. Geben Sie die URL des Datenfeeds ein: http://{dc-host}/Citrix/Monitor/OData/v2/Data (oder "https:", wenn Sie TLS verwenden). Falls erforderlich, geben Sie den Benutzernamen und das Kennwort für den Zugriff auf den Delivery Controller ein. Klicken Sie auf **OK**.
5. Sie können jetzt LINQ-Abfragen für den Datenfeed ausführen und die Daten nach Bedarf exportieren. Beispiel: Klicken Sie mit der rechten Maustaste auf "Catalogs" und wählen Sie **Catalogs.Take(100)** aus. Damit werden die ersten 100 Kataloge in der Datenbank zurückgegeben. Wählen Sie "Export > Export to Excel with formatting" aus.

Weitere funktionierende Beispiele für die Verwendung der API mit LINQPad finden Sie unter http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/.


© 1999-2017 Citrix Systems, Inc. All rights reserved.